




## LogRhythm Regulatory Compliance Support

Recent regulations governing specific industries and publicly traded companies have instituted standards for securing networks, systems, and data. A common thread throughout all regulations is a requirement to periodically review log data for the purpose of detecting intrusion, misuse, and fraud. Most regulations also require the implementation of intrusion detection systems, incident response procedures, and periodic reporting. Meeting these requirements can be time intensive and costly. By deploying LogRhythm, companies can immediately address and automate specific log data review, storage and retention requirements. LogRhythm’s Security Event Management capabilities provide a single centralized view of all security activity. LogRhythm’s automated analysis engines automate the process of detecting and alerting on suspicious activity. LogRhythm’s powerful forensic capabilities streamline the incident analysis & response process. For regulatory reporting requirements, LogRhythm includes one-click pre-packaged reports. The cost of deploying LogRhythm is typically recovered within a twelve month period or less due to the operational, security and audit efficiencies introduced.

### Affected Industries Matrix

The following chart lists the regulations affecting specific industries.


































Industry/Company Type	PCI	SOX	GLBA	HIPAA	FISMA
Publicly Traded Company	Yellow	Purple	Yellow	Yellow	Green
Banking & Financial Services	Yellow	Yellow	Purple	Green	Green
Insurance	Yellow	Yellow	Purple	Purple	Green
Health Care	Yellow	Yellow	Yellow	Purple	Green
Retail	Purple	Yellow	Yellow	Green	Green
Telecommunications/ISPs	Yellow	Yellow	Yellow	Green	Yellow
Energy	Yellow	Yellow	Yellow	Green	Yellow
Universities	Yellow	Green	Yellow	Yellow	Green
Defense Contractors	Yellow	Yellow	Green	Green	Purple
State and Local Agencies	Yellow	Green	Yellow	Yellow	Purple
Federal Agencies	Yellow	Green	Yellow	Yellow	Purple

-  Companies within the industry are directly affected and have specific compliance requirements
-  Companies within the industry may have compliance requirements
-  Companies within the industry are not affected

(Refer to Appendix A for an overview of each regulation)

## LogRhythm Compliance Checklist

The following chart lists the compliance areas addressed by LogRhythm within each regulation.

Compliance Requirement	Visa PCI	SOX	GLBA	HIPAA	FISMA
Log Data Centralization					
Log Data Archiving & Restoration					
System Integrity Monitoring					
Intrusion Detection					
Incident Response					
Periodic Log Review					
Audit Reporting					



**Implementing LogRhythm directly meets the requirement.**



**Using LogRhythm supports and reduces cost associated with meeting the requirement.**

## Explanation of LogRhythm Compliance Areas

### Periodic log review

Periodic log review consists of reviewing audit, system, and application logs on a regular basis for the purpose of detecting unauthorized activity and assessing the general health of systems and applications. LogRhythm significantly reduces the log review effort by automatically identifying high interest log events and detecting suspicious activity via rules and anomaly based log data analysis engines.

### Log data centralization and safeguarding

Log data centralizing and safeguarding consists of moving or copying log data to a centralized data store. The central data store can provide a secondary copy of log data and secure the log data from unauthorized access and modification. It also provides a means of analyzing log data across multiple systems simultaneously. LogRhythm provides agent and agent-less cross-platform log collection and secure log data centralization.

### **Log data archiving and destruction**

Log data archiving and destruction is the process of permanently destroying (deleting) log data or preparing log data for long term storage. Many standards require log data to be stored for months or even years before it can be destroyed. LogRhythm automates the process of destroying and archiving log data.

### **File Integrity Monitoring**

File integrity monitoring consists of monitoring the files on a system for read access, modification, deletion, and changes to access control settings. File integrity monitoring is typically accomplished via software that periodically checks systems for changes to sensitive files (e.g., password files, configuration files, programs). Monitoring the integrity of files is required by many standards for the purpose of detecting unauthorized changes to a system or its data. LogRhythm agents have built-in file integrity monitoring capabilities.

### **Intrusion detection**

Intrusion detection is the process of detecting intrusions into the network, systems, and applications whether the intruder is an external hacker or a disgruntled employee. Intrusion detection typically involves deploying network and host-based intrusion detection systems as well as reviewing the security logs of network devices, systems, and applications. LogRhythm can integrate with existing intrusion detection systems or be deployed with low-cost open source solutions such as Snort to create a much more effective multi-layer intrusion detection solution.

### **Incident response**

Incident response is the process of responding to and resolving an incident whether the incident be an intrusion or the failure of a critical financial system (e.g., general ledger application). Many standards require that formal incident response procedures be put in place and that tools exist for expediting and tracking the incident response process. LogRhythm provides advanced analysis and reporting tools to support and expedite the incident response process.

### **Reporting**

Reporting is the process of producing periodic reports on the integrity and security of the network, systems, and data. Reporting is required by many standards for the purpose of providing executives, managers, auditors, and other compliance related personnel a formal, written account of activity. LogRhythm automates the reporting process via its included reports and can be easily extended to meet custom reporting requirements.

## Appendix A

### Explanation of Regulations

**The Payment Card Industry (PCI) Data Security Standard (DSS)** was created by the leading credit card companies to ensure customer data is safeguarded. Visa, MasterCard and American Express require service providers and merchants that store, process, or transmit cardholder data to comply with the PCI Data Security Standard. The PCI Data Security Standard provides a single, uniform approach for securing and safeguarding sensitive customer data. Non-compliance can result in significant penalties and can include revocation of the company's right to accept or process credit card transactions.

**The Sarbanes Oxley Act (SOX)** of 2002 is a new and very widely publicized set of regulations governing corporate accountability, which requires strict internal IT controls and processes. It applies to all publicly traded companies. SOX Section 404 requires organizations identify "control deficiencies" that could affect the financial reporting of the company. Sarbanes Oxley recommends regular audits of log files and keeping a record of audit logs for up to seven years: "Audit unauthorized access, misuse and fraud, in order to ensure the accuracy of corporate financial and business information" and "maintain financial records for seven years."

**The Gramm-Leach-Bliley Act (GLBA)** requires that all institutions handling financial, non-public, or personal information to generate safeguards to protect this information. The act requires that the organizations implement an Information Security program and employ a coordinator to oversee the program. Information Security program audits should be reviewed by senior management on a regular basis to assure suitability of processes and implementation.

**The Health Insurance Portability and Accountability Act (HIPAA)** is a far-reaching federal law that requires hospitals, physicians, and managed care companies to adopt medical information security, privacy, and data standards. HIPAA requires organizations: audit and monitor system and user activity across the entire network, identify and investigate security breaches, and maintain a trail of user and network activity, They also specify companies retain and protect log data as evidence up to 6 years.

**The Federal Information Security Management Act (FISMA)** was signed into law in 2002. FISMA provides a framework for comprehensively securing federal information and assets. FISMA compliance is a matter of national security and applies to the information and associated systems used by federal agencies, contractors, and other organizations. FISMA includes standards and requirements for auditing, software and information integrity, intrusion detection, incident response, and reporting.

## Regulatory bodies and influencers

**Information Systems Audit and Control Association (ISACA)** is an international association recognized for their guidance and development of IS auditing and control standards. ISACA is well known for the development of COBIT, a generally accepted framework of control objectives and guidelines that help IT professionals implement information governance, control, and security.

**ISO 17799** is a globally recognized standard for information security. The framework requires companies to “review the results of the monitoring activities regularly,” and “maintain audit logs for system access and use, changes made, faults, corrective action, capacity demands and utilization.” ISO 17799 also states that organizations are obliged to ensure the accuracy of the logs.

**National Institute of Standards and Technology (NIST) 800-53** recommends Security Controls for Federal Information Systems. NIST suggests organization analyze logs specifically to identify points of performance, suspicious login activity, general use activity and software installation.

The **CERT Coordination Center**, a center of Internet security expertise, recommends companies document a management plan for handling log files, analyze the log files on a periodic basis to look for suspicious behavior. CERT also recommends companies consolidate and retain the log files at a central location in a secure and reliable manner to provide post-incident information and audit trail.

**National Industrial Security Program Operating Manual (NISPOM)**, developed by the Department of Defense and Department of Energy, recommends that companies should analyze log and audit data on a weekly basis. The manual recommends that organizations create a granular, automated audit trail and should include monitoring of login and file access attempts and failures. NISPOM also recommends that activity logs be secured and retained for a minimum of one year.

**Public Company Accounting Oversight Board (PCAOB)** Audit of Internal Control standard provides a road map for creating a defensible and auditable set of security controls for public companies. PCAOB requires steps to prevent or detect theft, unauthorized use, or disposition of the company’s assets that could have a material effect on financial statements.

**SANS (SysAdmin, Audit, Network, Security)** Institute is a cooperative research and education organization and the largest source for information security training and certification in the world. SANS emphasizes the importance of maintaining a thorough audit trail to facilitate security breaches and other unexplainable behavior. They also suggest companies regularly rotate log data, archiving older data.