LogRhythm Support for ISO 27001

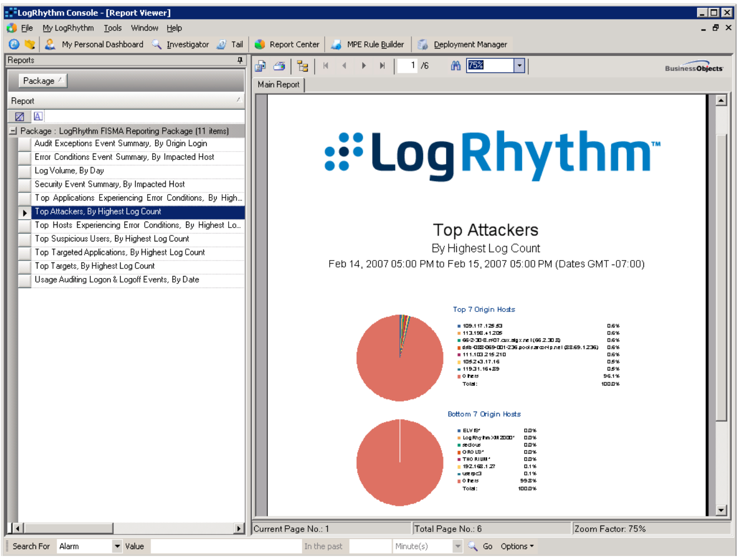
LogRhythm Support for ISO 27001

ISO (International Organization for Standardization) Standard 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS (Information Security Management System) within the context of the organization's overall business risks. These published guidelines cover many areas surrounding "access control", "audit and accountability", "incident response", and "system and information integrity".

The collection, management, and analysis of log data are integral to meeting many ISO 27001 guidelines. The use of LogRhythm directly meets some recommendations and decreases the cost to meet 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. The additional recommendations of analyzing and reporting on log data render manual processes or homegrown remedies inadequate and cost prohibitive for many organizations.

LogRhythm delivers log collection, archiving, and recovery across the entire IT infrastructure and automates the first level of log analysis. Log data is categorized, identified, and normalized for easy analysis and reporting. LogRhythm's powerful alerting capabilities automatically identify the most critical issues and notify relevant personnel. With the click of a mouse or via an automated scheduler, LogRhythm's out-of-the box ISO 27001 reporting packages ensure you meet your reporting needs.

ISO 27001 and its recommendations guide organizations to implement and perform procedures to effectively capture, monitor, review and retain log data. The remainder of this paper lists the applicable ISO control guidelines, as specified in Instruction 8500.2, that LogRhythm helps address. For each recommendation, an explanation of how LogRhythm support the guideline is provided. Learn how LogRhythm's comprehensive log management and analysis solution can help your organization meet or exceed ISO 27001 guidelines.



Package : LogRhythm FISMA Reporting Package (11 items)

- Audit Exceptions Event Summary, By Origin Login
- Error Conditions Event Summary, By Impacted Host
- Log Volume, By Day
- Security Event Summary, By Impacted Host
- Top Applications Experiencing Error Conditions, By High...
- Top Attackers, By Highest Log Count
- Top Hosts Experiencing Error Conditions, By Highest Lo...
- Top Suspicious Users, By Highest Log Count
- Top Targeted Applications, By Highest Log Count
- Top Targets, By Highest Log Count
- Usage Auditing Logon & Logoff Events, By Date

Top Attackers
By Highest Log Count
Feb 14, 2007 05:00 PM to Feb 15, 2007 05:00 PM (Dates GMT -07:00)

Top 7 Origin Hosts

109.117.129.53	0.6%
113.198.41.205	0.6%
66-2-30-8.sf07.cux.algx.net (66.2.30.8)	0.6%
dslb-088-069-001-236.pools.arcor-ip.net (88.69.1.236)	0.6%
111.103.215.210	0.6%
105.243.17.16	0.5%
119.31.164.89	0.5%
Others	96.1%
Total:	100.0%

Bottom 7 Origin Hosts

ELVIS*	0.0%
LogRhythmXM2000*	0.0%
sedous	0.0%
GROLS*	0.0%
THORIUM*	0.0%
192.168.1.27	0.1%
userpc3	0.1%
Others	99.8%
Total:	100.0%

Current Page No.: 1 | Total Page No.: 6 | Zoom Factor: 75%

LogRhythm Report Center Screenshot

A.6 Organization of Information Security

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.6.1.3 Allocation of Information Security Responsibilities	All information security responsibilities shall be clearly defined.	LogRhythm can divvy up tasks and keep log information organized through restricted analysts and alarm viewers. LogRhythm can track an alarm status, delegate it to someone, change its current state (working, escalated), and add comments. **Example Reports:** • Alarm And Response Activity • Alarms With Event And Activity Detail • Usage Auditing Activity Summary

A.8 Human Resource Security

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.8.3.3 Removal of Access Rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	LogRhythm collects all account management activities. LogRhythm reports provide easy and standard review of all account management activity. **Example Reports:** • Account Management Activity • Terminated Account Summary

A.10 Communications and Operations Management

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.10.1.2 Change Management	Changes to information processing facilities and systems shall be controlled.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitoring Log Detail • File Integrity Monitor Log Summary • Patches Applied • *NIX Hosts Configuration Changes • Windows Hosts Configuration Changes
A.10.3.1 Capacity Management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	LogRhythm provides central, secure, and independent audit log storage. LogRhythm's central and extensible storage of audit log data ensures capacity will not be exceeded. 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's alarming capability can be used to independently detect and alert on threshold violations. **Example Reports:** • Log Volume (By Log Source) • System Critical And Error Conditions • *NIX Hosts Critical Events and Errors • Windows Hosts Critical Events And Errors

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.10.3.2 System Acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.	LogRhythm can track and report on when patches are installed on devices, showing which systems have had patching within the past month, or any other time frame as dictated by organizational policy. **Example Reports:** • Patches Applied
A.10.4.1 Controls Against Malicious Code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	LogRhythm detects and alerts on any error conditions originating from anti-virus applications, when the services are started and stopped, as well as identifies when new signatures are installed. Alarming can be configured to inform the custodian(s) of when any malware is detected inside the environment. **Example Reports:** • Anti-Virus Signature Update Report
A.10.5.1 Information Back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	LogRhythm can track and report on when backups are performed within the past month, or any other time frame as dictated by organizational policy. **Example Reports:** • Backup Status
A.10.6.1 Network Controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	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. **Example Reports:** • Network Device Critical Events And Errors • Network Device Configuration Changes • *NIX Hosts Configuration Changes • Windows Hosts Configuration Changes • Security Device Policy And Configuration **Example Alarms:** • Network Device Critical Condition
A.10.8.4 Electronic Messaging	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	LogRhythm provides a record of all services used and can alarm on the use of non-encrypted protocols. **Example Reports:** • Use Of Non-Encrypted Protocols
A.10.9.3 Publicly Available Information	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitoring Log Detail
A.10.10.1 Audit Logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	LogRhythm completely automates the process and requirement of collecting and retaining security event logs. LogRhythm retains logs in compressed archive files for cost effective, easy to-manage, long-term storage. Log archives can be restored quickly and easily months or years later in support of after-the-fact investigations. **Example Reports:** • Log Volume (By Log Source) **Example Alarms:** • LogRhythm Silent Log Source Error

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.10.10.2 Monitoring System Use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	LogRhythm's monitoring, analysis, archiving, alerting, auditing, and reporting capabilities provide for continuous monitoring of access points across the Electronic Security Perimeter(s). For instance, LogRhythm monitors unauthorized access for auditing, logging, archiving, and alerting. **Example Reports:** • Alarm And Response Activity • Usage Auditing Event Detail (By User)
A.10.10.3 Protection of Log Information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Using LogRhythm helps ensure audit trails 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. **Example Reports:** • Access Failures By Login • Login Failures By Login
A.10.10.5 Fault Logging	Faults shall be logged, analyzed, and appropriate action taken.	LogRhythm collects logs continuously and real-time in the organizational IT environment. The logs are normalized, analyzed and presented in the LogRhythm Dashboard for real-time review. Alarms are activated on critical events that will cause immediate and direct notification to the administration. Reports and investigations for compliance are available at all times. **Example Reports:** • System Critical And Error Conditions • Alarm And Response Activity • Usage Auditing Activity Summary

A.11 Access Control

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.11.2.1 User Registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	LogRhythm collects all account management and account usage activity. Changes to accounts, usage of default accounts and the full gamut of authorization and permissions related activity are automatically monitored and can be easily alerted on when nefarious unauthorized activity is detected. Packaged reports are provided to supply full account of all account usage and change history. **Example Reports:** • Account Management Activity • Host Access Granted And Revoked
A.11.5.1 Secure Log-on Procedures	Access to operating systems shall be controlled by a secure log-on procedure.	LogRhythm collects all account management and account usage activity. Changes to accounts, usage of default accounts and the full gamut of authorization and permissions related activity are automatically monitored and can be easily alerted on when nefarious unauthorized activity is detected. Packaged reports are provided to supply full account of all account usage and change history. **Example Reports:** • Administrative Authentication Summary • User Authentication Summary • Host Authentication Summary

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.11.5.4 Use of System Utilities	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	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:** • File Integrity Monitoring Log Detail • Processes By User
A.11.6.1 Information Access	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	LogRhythm supplies a one stop repository from which to review log data from across the entire IT infrastructure. Reports can be generated and distributed automatically on a daily basis. LogRhythm provides an audit trail of who did what within LogRhythm and a report which can be provided to show proof of log data review. **Example Reports:** • Access Failures By Login • Processes By User

A.12 Information Systems Acquisition, Development, and Maintenance

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.12.4.2 Protection of System Test Data	Test data shall be selected carefully, and protected and controlled.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.
A.12.4.3 Access Control to Program Source Code	Access to program source code shall be restricted.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitoring Log Detail
A.12.5.1 Change Control Procedures	The implementation of changes shall be controlled by the use of formal change control procedures.	LogRhythm monitors for proper operations and configuration changes that may jeopardize the security of the system. **Example Reports:** • Configuration Change Summary
A.12.5.2 Technical Review of Applications After Operating System Changes	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	LogRhythm monitors for proper operations and configuration changes that may jeopardize the security of cardholder data. **Example Reports:** • Configuration Change Summary
A.12.5.3 Restrictions on Changes to Software Packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	LogRhythm monitors for proper operations and configuration changes that may jeopardize the security of cardholder data. **Example Reports:** • Configuration Change Summary

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.12.5.4 Information Leakage	Opportunities for information leakage shall be prevented.	LogRhythm's Data Loss Defender (DLD) feature independently monitors and logs the connection and disconnection of external data devices to the host computer where the Agent is running. It also monitors and logs the transmission of files to an external storage device. **Example Reports:** • LogRhythm Data Loss Defender Log Detail
A.12.6.1 Control of Technical Vulnerabilities	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	Vulnerabilities can be detected by real-time examination tools or by using compatible vulnerability scanning systems. Alarming can be configured to inform the custodian(s) of when any malware is detected inside the environment. **Example Reports:** • Vulnerabilities Detected • Malware Detected **Example Alarms:** • Alarm on Malware

A.13 Information Security Incident Management

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.13.1.1 Reporting Information Security Events	Information security events shall be reported through appropriate management channels as quickly as possible.	Vulnerabilities can be detected by real-time examination tools or by using compatible vulnerability scanning systems. Alarming can be configured to inform the custodian(s) of when any malware is detected inside the environment. **Example Reports:** • Vulnerabilities Detected • Malware Detected **Example Alarms:** • Alarm on Malware
A.13.1.2 Reporting Security Weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	LogRhythm documents alarm and response activities such as 'responsible parties notified'; alarm status such as 'working, escalated, resolved'; and what actions were taken. **Example Reports:** • Alarm And Response Activity
A.13.2.1 Responsibilities and Procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	LogRhythm documents alarm and response activities such as 'responsible parties notified'; alarm status such as 'working, escalated, resolved'; and what actions were taken. **Example Reports:** • Alarm And Response Activity
A.13.2.2 Learning from Information Security Incidents	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	LogRhythm completely automates the process and requirement of collecting and retaining security event logs. LogRhythm retains logs in compressed archive files for cost effective, easy to-manage, long-term storage. Log archives can be restored quickly and easily months or years later in support of after-the-fact investigations. **Example Reports:** • Log Volume (By Log Source) • Event Rate Analysis

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.13.2.3 Collection of Evidence	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	LogRhythm documents alarm and response activities such as 'responsible parties notified'; alarm status such as 'working, escalated, resolved'; and what actions were taken. **Example Reports:** • Alarm And Response Activity

A.14 Business Continuity Management

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.14.1.2 Business Continuity and Risk Assessment	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.	LogRhythm collects logs continuously and real-time in the organizational IT environment. The logs are normalized, analyzed and presented in the LogRhythm Dashboard for real-time review. Alarms are activated on critical events that will cause immediate and direct notification to the administration. Reports and investigations for compliance are available at all times. **Example Reports:** • System Critical And Error Conditions **ExamplÏe Alarms:** • Windows Host Critical Condition • *NIX Host Critical Condition

A.15 Compliance

ISO 27001 Compliance Recommendation		How LogRhythm Supports the Guideline
A.15.1.3 Protection of Organizational Records	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitoring Log Detail
A.15.3.2 Protection of Information Systems Audit Tools	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitoring Log Detail