THE LOGRHYTHM SOX COMPLIANCE AUTOMATION MODULE:
SOX Compliance Made Easy
Table of Contents

3  SOX Compliance at a Glance

3  LogRhythm Provides Automated Compliance Support for SOX

3  SOX Compliance Automation Module Benefits:

4  The LogRhythm SOX Compliance Automation Module
   4  Incorporating Risk Assessment Results
   4  Detecting and Stopping Threats
   5  Facilitating Investigations and Reporting
   5  Monitoring IT Operations and Change Control Processes

6  ITGC Breadth and Depth

6  Areas of SOX Supported by LogRhythm

7  Conclusion
The Sarbanes-Oxley Act of 2002, better known as SOX, was created to ensure the completeness and accuracy of financial reports from publicly traded companies in the United States. Prior to SOX, several U.S. companies were caught in major scandals for using fraudulent accounting practices. These scandals involved huge financial losses and far-reaching negative repercussions for shareholders and many other parties. Ultimately, SOX established controls to detect and stop similar wrongdoing in the future.

All publicly traded companies, as well as those organizations in the process of going public or considering going public, must adhere to all SOX compliance requirements. This includes establishing, monitoring, and maintaining a wide range of information technology (IT) security controls, as well as policies to demonstrate controls adhere to SOX requirements. Fortunately, there's a solution that can save you a great deal of time in meeting and exceeding compliance requirements: the LogRhythm SOX Compliance Automation Module.

SOX Compliance at a Glance
SOX defines a broad set of requirements that include three types of internal controls related to financial reporting: financial, operational, and IT. These controls work together to help ensure the integrity of a company's financial reporting processes. They also hold individuals and the company accountable for any failures of integrity in financial reports. SOX compliance requirements apply to all parts of a company involved in financial reporting, including IT systems and networks.

A company planning to go public must also plan for SOX compliance. In what’s commonly called the SOX Readiness Phase, a company usually needs between two and four years to perform a risk assessment, prioritize its SOX compliance objectives, and select and implement the necessary financial, operational, and IT controls. Once the company goes public, it has one fiscal year to have an audit performed and to remediate the findings from the initial audit. At the end of that fiscal year, the company must be fully SOX compliant.

The U.S. Securities and Exchange Commission (SEC)—the high-level body overseeing SOX compliance—has the authority to penalize companies for non-compliance with SOX. Most penalties involve fines against the company, but in extreme cases, the SEC can impose prison sentences or hefty financial penalties on executives. In addition, non-compliance may expose companies to potential lawsuits and to significant damage to their reputations.

There are other entities with important roles in SOX compliance. For example, the Public Company Accounting Oversight Board (PCAOB) develops the audit standards for all the controls needed for SOX compliance. Also, there are many internal and external auditors who perform the actual SOX compliance audits, known as attestations.

LogRhythm Provides Automated Compliance Support for SOX
The LogRhythm SOX Compliance Automation Module helps ensure your company meets or exceeds the SOX compliance requirements for Information and Technology General Controls (ITGCs). Using the module significantly reduces risk for your financial reporting assets and assists your company in avoiding compliance violations and fines while also saving you time and money.

SOX Compliance Automation Module Benefits:
• Ability to utilize risk assessment results to improve the efficiency of incident investigations and responses
• Pre-built AI Engine rules and alerts mapped to numerous COBIT 5 practices and four major SOX control families
• Automation capabilities that minimize the manual effort usually needed to continuously monitor systems for signs of possible violations, including change control issues, and immediately respond to them
• Extensive security automation and orchestration (SAO) features that provide support throughout the entire threat life cycle management framework
• Predefined reports to easily document evidence of SOX compliance
In terms of IT controls, SOX only defines high-level requirements. SOX is meant to work in conjunction with a control framework that specifically lists the controls needed to mitigate risk and meet the SOX requirements. These controls are known as the Information and Technology General Controls (ITGCs). Over the years, various organizations have developed and refined more detailed control frameworks. One of these, Control Objectives for Information and Related Technologies edition 5 (COBIT 5), has replaced COSO as the ITGC framework for SOX.

Complying with COBIT 5’s requirements for ITGCs requires a highly automated approach. Logs from many systems throughout the company need to be brought together, monitored, and analyzed continuously in order to quickly identify any security-related issues and to meet SOX compliance requirements. Without robust enterprise log management capabilities that are SOX-savvy, any company will find it incredibly time-consuming and expensive to attest that its ITGCs are SOX compliant. This is where the LogRhythm SOX Compliance Automation Module comes in.

### The LogRhythm SOX Compliance Automation Module

The LogRhythm SOX Compliance Automation Module enables your company to meet or exceed SOX requirements for ITGCs. This helps your company to avoid compliance violations and fines and significantly reduce risk for its IT assets involved in financial reporting. The compliance module is available to all LogRhythm customers free of charge.

Downloading and deploying the compliance module can give your company immediate benefits. The compliance module is developed, actively maintained, and refined by experts from LogRhythm Labs. LogRhythm Labs engineers do extensive research into SOX-mandated ITGCs and develop or update the necessary content for the compliance module. Examples of this pre-built content include AI Engine rules and alerts, dashboards, and reports. This content works in conjunction with existing LogRhythm capabilities to give you a unified vantage point for all your SOX compliance efforts involving ITGCs. To see a full list of content, please refer to the LogRhythm SOX Compliance Automation Module User Guide.

The latest release of the compliance module transitions companies from the COSO to the COBIT 5 framework. The compliance module is designed to save your company time when tailoring your LogRhythm deployment to meet SOX mandates. The module also automates a great deal of the necessary SOX ITGC compliance work so as to minimize the manual workload on your company's staff. Let’s look at the most important capabilities the module can provide to your company.

### Incorporating Risk Assessment Results

Risk assessment is the foundation of a SOX compliance program. Your company can't achieve SOX compliance without first having a clear understanding of the risks involving your organization's business and IT assets used for financial reporting. These assets include accounting systems and enterprise resource planning (ERP) systems, supporting production systems such as backup servers and authentication servers, and even test systems. Risk assessment results for these assets are invaluable inputs to LogRhythm and its SOX compliance module. LogRhythm can use the results to improve the efficiency of incident investigation and responses, such as by assigning a higher priority to a security event on a higher-risk system than the same event on a lower-risk system. LogRhythm can use the risk levels in other ways as well (e.g., performing more detailed logging for events occurring on a higher-risk system).

### Detecting and Stopping Threats

The LogRhythm SOX Compliance Automation Module offers a wide range of capabilities for detecting and stopping threats. The compliance module has many built-in SOX rules that will generate alerts to notify administrators of possible violations of SOX requirements.

User access management is one area of threat detection where the compliance module is particularly helpful. SOX and COBIT 5 emphasize the importance of continuously monitoring all account usage within the relevant systems—particularly for accounts with administrator privileges and accounts used by vendors and other third parties. By automatically defining and maintaining lists of the user accounts to monitor, such as through Active Directory Sync, LogRhythm can monitor all actions performed by these accounts as they occur. The SOX Compliance Automation Module quickly identifies issues with how these accounts are being used so the necessary response can be initiated immediately. The compliance module also enables people to easily conduct periodic access reviews to make sure each account is still needed. This is particularly important for ensuring that vendor access has been terminated when their contracts end.
The compliance module has many other capabilities for threat detection. One example is its ability to ingest, analyze, and correlate events within and across file integrity monitoring logs. This could identify someone tampering with operating system executables or application log files in order to alter financial system audit records. Another example of the compliance module's capabilities is its data loss prevention features. The module includes rules that look for unusual patterns of attempts to access sensitive data or to transfer that data to unexpected or unauthorized locations. Through these rules, the module can detect exfiltration attempts and alert administrators to intervene immediately.

Facilitating Investigations and Reporting
Incident management and response are major priorities under SOX. LogRhythm offers extensive security automation and orchestration capabilities, including case management, that provide support throughout the entire threat lifecycle management framework. The LogRhythm SOX Compliance Automation Module adds to those by providing the following:

- Sets of pre-built rules constantly monitor data to log evidence of SOX compliance and identify and record information on potential SOX violations and other issues.
- Pre-built SOX dashboards bring together and present forensic data in support of incident investigations.
- A SOX reporting package makes it easy to get the right information to the right people quickly. The package offers a variety of fully automated SOX compliance reports for all levels of management. The reports encompass not only incident-related information, but also all other information needed to identify issues with SOX compliance and to provide evidence to auditors and others of SOX compliance.

LogRhythm’s SOX Compliance Automation Module provides all the necessary information for analysts to make sound strategic decisions regarding incidents. It also captures forensic evidence of incident mitigation and recovery actions, which is needed to demonstrate that security weaknesses and other issues were remediated to prevent recurrences of the same problem.

Monitoring IT Operations and Change Control Processes
In addition to having many purely security-related requirements, SOX has requirements related to IT operations and change control, because these areas can have significant impacts on security. The most basic need is to continuously monitor the relevant systems for critical errors that require attention. An example is a major failure of a system’s audit functions or backup capabilities. The compliance module provides continuous monitoring and can alert administrators to immediately respond to problems that may negatively impact SOX compliance.

In terms of change control, the compliance module continuously monitors all change control activities, such as patch deployment, attack signature distribution, and system configuration changes. This helps ensure that all such changes are properly approved before they are implemented. The compliance module also looks for violations of separation of duties related to change control, such as an individual making changes to a configuration in the test environment and immediately migrating those changes to the production environment. SOX requires adherence to formal change control processes, including performing an impact analysis for each change planned for production, so the compliance module can identify attempts to circumvent those processes.

LogRhythm enables us to spend less time staring at screens trying to review logs—leading to increased visibility and productivity.

— Marc White, CISO, Optomany, LTD
ITGC Breadth and Depth

The table below summarizes how the LogRhythm SOX Compliance Automation Module's capabilities support numerous COBIT 5 practices that map to four major SOX control families. This may look like a large number of practices for your company to have perfectly mastered as of day one of your SOX compliance efforts. The good news is the expectation with SOX and the compliance module is that your company’s ITGCs will mature over time, both in terms of adding controls and in adjusting existing controls to meet more stringent requirements. LogRhythm Labs has designed the compliance module to benefit your organization at any compliance maturity level. The compliance module is built to be adaptable as your company, its security needs, and its IT environment and infrastructure change.

Areas of SOX Supported by LogRhythm

<table>
<thead>
<tr>
<th>SOX Control Family</th>
<th>Corresponding COBIT 5 Practices Supported by the LogRhythm SOX Compliance Automation Module</th>
<th>LogRhythm SOX Compliance Automation Module Capabilities</th>
</tr>
</thead>
</table>
| Align, Plan, and Organize (APO - IT Environment) | • Manage the IT Management Framework [APO01]  
• Manage Strategy [APO02]  
• Manage Human Resources [APO07]  
• Manage Service Agreements [APO09]  
• Manage Suppliers [APO10] | • Detecting and Stopping Threats  
• Facilitating Investigations and Reporting |
| Build, Acquire, and Implement (BAI - Programme Development and Programme Change) | • Manage Solutions Identification and Build [BAI03]  
• Manage Availability and Capacity [BAI04]  
• Manage Changes [BAI06]  
• Manage Change Acceptance and Transitioning [BAI07]  
• Manage Configuration [BAI10] | • Incorporating Risk Assessment Results  
• Monitoring IT Operations and Change Control Processes |
| Deliver, Service and Support (DSS - Operations and Access to Programmes and Data) | • Manage Operations [DSS01]  
• Manage Service Requests and Incidents [DSS02]  
• Manage Problems [DSS03]  
• Manage Continuity [DSS04]  
• Manage Security Services [DSS05]  
• Manage Business Process Controls [DSS06] | • Detecting and Stopping Threats  
• Facilitating Investigations and Reporting |
| Monitor, Evaluate and Assess (MEA - IT Environment) | • Monitor, Evaluate and Assess Performance and Conformance [MEA01] | • Facilitating Investigations and Reporting |

To see a full list of controls, please refer to the LogRhythm SOX Compliance Automation Module User Guide.
Conclusion

LogRhythm’s innate capabilities strongly support security controls in general by bringing together logs from throughout a company and continuously monitoring, analyzing, and correlating security-related events within those logs. This enables LogRhythm to identify attacks, compromises, and other security issues, as well as help verify that technical controls are in place and functioning as expected. LogRhythm also offers superior security automation and orchestration features that cover the entire threat lifecycle management framework, making it easy to track the status of any incident and see all related data in one place.

SOX requires companies to employ a wide range of ITGCs based on COBIT 5 practices. The LogRhythm SOX Compliance Automation Module builds on LogRhythm’s existing features to enable your company to meet or exceed its SOX ITGC requirements. The compliance module provides a comprehensive, pre-built set of rules, alerts, dashboards, and reports specifically designed for achieving SOX compliance. The LogRhythm platform and the compliance module work together to provide a fully integrated solution for your company’s SOX needs. Unique capabilities the solution provides include the following:

- Incorporating risk assessment results, such as prioritizing incident investigations and responses for certain assets
- Detecting and stopping threats, from identifying issues with how user accounts are being used to detecting system file tampering and data exfiltration attempts
- Facilitating investigations and reporting by supporting the entire threat lifecycle management framework through logging, dashboards, and compliance reports
- Monitoring IT operations and change control processes for issues with security implications

With LogRhythm, you don’t have to start from scratch to achieve SOX compliance. The experts at LogRhythm Labs developed the compliance module based on extensive research into SOX ITGCs, first with COSO and now with COBIT 5. LogRhythm provides this embedded expertise so your company can download the compliance module, define the relevant systems and data, tweak the module’s configuration for your environment, and start using the module immediately. This starts your company on a much faster path to demonstrating SOX compliance and saves your staff a great deal of time and effort. By meeting or exceeding SOX ITGC requirements, your company will lower its risk, accelerate incident detection and management, and reduce the likelihood of having significant compliance violations.

For more information on how LogRhythm’s SOX Compliance Automation Module can benefit your company, schedule a demo at www.logrhythm.com/schedule-online-demo/.
About LogRhythm
LogRhythm, a leader in Threat Lifecycle Management, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyberthreats. The company’s patented award-winning platform unifies next-generation SIEM, log management, network and endpoint monitoring, user entity and behavior analytics (UEBA), security automation and orchestration (SAO) and advanced security analytics.

In addition to protecting customers from the risks associated with cyberthreats, LogRhythm provides compliance automation and assurance, and enhanced IT intelligence.

Among its many industry accolades, LogRhythm has been positioned as a Leader in Gartner’s SIEM Magic Quadrant, received SC Labs’ “Recommended” rating for SIEM and UTM for 2017 and won “Best SIEM” in SANS Institute’s “Best of 2016 Awards.”