White Paper

Complying with SOX Regulations Using the Exabeam Security Intelligence Platform

exabeam

INTRODUCTION

The Sarbanes-Oxley Act (SOX) was born from the ashes of major financial scandals involving such corporate giants as Enron, Arthur Andersen, Tyco, and WorldCom. Established in 2002, SOX is viewed as one of the most far-reaching pieces of U.S. securities legislation since the 1930s. Created to restore shareholder faith in public corporations, it has set forth mandates for the reliability of financial reporting.

For corporations, achieving compliance involves many people across multiple teams. Information security professionals play a key role in a company's SOX compliance. Subsequently amended to include cybersecurity considerations, it recognizes the increasing importance of protecting people, systems, and data in pursuit of fair and transparent financial reporting.

SOX OVERVIEW AND GOVERNANCE

SOX has considerable enforcement muscle to drive compliance. The U.S. Securities and Exchange Commission (SEC) has the authority to impose heavy fines for non-compliance—and even imprisonment for executives whose companies run afoul. Along with that comes reputational damage from having violated the law. Losing faith with shareholders, a corporation may have to expend a significant amount of resources in rebuilding it. Further, lawsuits against corporations found to be in non-compliance are not uncommon.

PCAOB – The SEC is not the only important entity involved. The Public Company Accounting Oversight Board (PCAOB) oversees the auditing of public companies. It sets the rules and standards for audit reports, with all firms that audit public companies having to be PCAOB-registered. Auditors look to it for training and best practices in evaluating internal corporate controls; knowing the latest PCAOB guidelines is essential to passing an audit assessment. The board also has the authority to inspect, investigate, and enforce all compliance overseen by its registrants.

COBIT – Given the complexity of SOX, entities specifically related to IT controls have arisen. To help companies map out their compliance, ISACA developed COBIT (originally Control Objectives for Information and Related Technology) as a globally-accepted framework of best practices for thirty-four IT processes. COBIT 5 is the latest and most detailed version.

ITGC – Narrowing this down even further, the Information Technology Governance Institute publishes a framework that draws from COBIT, but focuses solely on security issues. Its Information and Technology General Controls help bring focus and actionability to SOX's broad requirements.

SOX AND THE SPECIFIC IT SECURITY ROLE

SOX regulations touch every aspect of financial reporting, including IT systems that support it. The latter are directly involved in collecting and storing data, in addition to verifying its accuracy. Operational and financial controls are not enough—IT controls are inextricably linked, especially since most records are digital. Therefore the integrity of any reporting rests on the IT backbone; operations teams play a critical role in holding the corporation accountable.

Protecting IT systems is essential. A 2016 bill modified the rules, specifically referring to "cybersecurity systems" alongside standard financial systems and practices. As a result SOX now contains two notable sections pertaining to cybersecurity:

- **Section 302** – Pertains to corporate responsibility for financial reports. It requires systems that protect against data tampering—whether from a malicious insider or an external hacker making use of stolen credentials. SOX does not prescribe how such protection must occur, but it does require the ability to track timelines and determine the who-what-when of data access. Periodic statutory financial reports by a corporation must also certify any changes and/or deficiencies in controls, as well as report any data breaches.
- **Section 404** – Addresses managerial evaluation of internal controls. A corporation must assess them (including IT controls) in an annual SEC report, also providing the results to an external (unbiased) audit firm. Section 404 focuses on transparency and requires all data be made available to auditors, such that they can independently verify security system efficacy. Potential data breaches must be disclosed. As with Section 302, SOX does not provide specific guidance as to which controls should be assessed.

Achieving full SOX compliance will always require strong security systems to be in place. This includes, but is not limited to:

- monitoring logs and security events
- ensuring proper access and credential use
- creating protection against data tampering and loss
- implementing strong incident response mechanisms
- incorporating risk assessment results

HOW EXABEAM CAN HELP

Exabeam's Security Intelligence Platform offers a host of supportive SOX compliance capabilities. Its technology provides transparency and detailed oversight of user and entity behavior. This level of visibility helps IT security teams quickly evaluate any system integrity threats, including unauthorized access. And it doesn't stop there. To assist security teams in mitigating actual threats, Exabeam provides robust incident response capabilities and automated playbooks. Our platform provides corporations with the tools required to support extensive, SOX-compliant financial reporting.

Security Event Monitoring, Including Sensitive File Access

Log and event monitoring is at the core of diligent information security. IT teams use security intelligence platforms, such as Exabeam, to ingest—directly or via a SIEM/log management system—file access logs, Windows® event logs, email logs, web proxy logs, and other data to identify risky activity related to financial reporting. Depending on infrastructure size, a considerable amount of event information may be collected. Here, Exabeam's data lake can manage an unlimited load without the corporation being charged for additional data storage.

To detect data tampering, Exabeam has built-in file monitoring models that track every file-related action—including initial access, attaching data to an email, downloading, or even writing to a USB drive—even as a user changes devices or account identities. For example, if an employee copies a sensitive file to a workstation, then attaches

it to an email using an unrelated, shared admin account, Exabeam can confidently attribute such an activity chain to that person. Many of Exabeam's models are context-based; it understands that even an authorized user, accessing files outside of their normal baseline activity, can be a red flag. Within the context of SOX, Exabeam can detect and flag an unauthorized user who has accessed a folder owned by an organization's CxO.

Exabeam is able to ingest log information across different threat vectors (e.g., cloud, database, email, application) and assemble it into a coherent activity chain—even as users try to hide by swapping account credentials, devices, or IP addresses.

Detects Compromised Credentials

Ensuring that only authorized personnel have access to sensitive data is a fundamental control for financial reporting systems. Its scope includes preventing unauthorized, internal employees—as well as external actors—from obtaining credentials and initiating an attack chain. Both SOX and COBIT 5 emphasize the importance of continuous account monitoring, especially that of privileged users and third-party vendors who have special access. But such credential use can appear as legitimate business, resulting in malicious activity potentially going unnoticed.

Exabeam eliminates this problem by detecting anomalies and constructing a complete dossier. It does so by accurately modeling the behavior of users, entities, and even alerts from other security solutions. It can quickly detect complex threats and alert teams about suspicious activity—even that which occurs through seemingly valid credential use. Being able to reveal anomalous activity in this way, Exabeam provides the context for security teams to take quick, decisive action.

Enables Rapid Investigation

SOX Section 302 requires organizations to implement systems that protect against data tampering, track timelines, and evaluate the who-what-when of data access. For insider threats, especially those involving lateral movement, it may be difficult and time-consuming—if not "impossible"—to create accurate incident timelines. But the Exabeam Security Intelligence Platform leverages user and entity behavior analytics to identify incidents, then automatically creates pre-built timelines to document them. While taking the burden off of limited human resources, such automation also helps fulfil the Section 302 requirement.

Effective Incident Response

Prevention is a core tenet of SOX, and it has historically been the focal point for IT security. But threats do occur, and incident management is a top priority. Exabeam has created an off-the-shelf incident response solution that automates tedious, manual tasks—freeing security teams to work on more important, value-add activities.

Exabeam's comprehensive security orchestration includes:

- Native integration with popular log management systems, security data lakes, and UEBA tools, enabling teams to quickly and easily initiate and manage breach investigations.
- Pre-built API integrations that can programmatically pull data from, or push actions to, hundreds of third-party IT and security infrastructure solutions. This enables visibility and rapid investigation for enterprise security and SOX-compliance stakeholders.

- Automated response workflows that leverage existing security solutions. These range from being passive (analyst notification), informational (warning emailed to an employee), to full force (access lock down and response instigation).

Exabeam's easy-to-use, intuitive interface enables even junior analysts to understand and take action on threats. Unlike existing triage and case management systems used by most SOCs to track incident statuses, Exabeam Incident Responder uses security orchestration and workflow automation. By leveraging API integration with IT infrastructure and security solutions, Exabeam can investigate, contain, and mitigate security incidents in a semi- or fully automated manner.

Incident response teams enjoy huge productivity gains, as Exabeam yields shorter response times and fewer manual errors. All security incidents are logged, providing forensic evidence that a corporation has taken steps to identify and remediate them.

Leveraging Risk Scores

SOX requires that corporations assess financial reporting risks and develop strong internal controls. This involves evaluating business and IT reporting assets, as well as assigning a meaningful risk score to each potential threat vector. Risk scores for a corporation's accounting systems, enterprise resource planning (ERP) systems, et al., are valuable data points Exabeam can use to inform incident response. When security events occur, for example, higher priority can be assigned to a critical financial system versus a lower-risk system.

Customizable Compliance Reporting

Exabeam helps with SOX Section 404 adherence, which requires organizations to report their regulation compliance annually. Our fully customizable reporting module makes it easy to create custom visualizations, dashboards, and reports to satisfy auditors.

Ensuring Effectiveness of Security Controls

Building a strong security posture is akin to creating an effective compliance program; there is no silver bullet. Instead it is the result of many people, processes, and technologies working together to achieve the same goal.

Exabeam provides a second defense layer by helping to ensure that people, processes, and products—functioning as security controls—are operating in unison. If a system is misconfigured, thus introducing undesired exposure and risk, Exabeam's behavioral analytics help detect and clearly identify it.

Monitoring IT Operations and Change Control Processes

Along with the many SOX requirements that are purely security-related, several pertain to IT operations and change control, as these can have a significant security impact. SOX requires adherence to formal change control processes, including an impact analysis for every production change. As IT environment changes occur, Exabeam's powerful combination of log management and data lake are continuously monitoring, logging, and reporting. Such a long-term data repository meets SOX auditing requirements, and compliance teams can quickly identify attempts to circumvent the change control process. Additionally, the Exabeam platform can alert administrators to immediately respond to critical errors that may negatively impact SOX compliance.

HOW EXABEAM MAPS TO SOX REQUIREMENTS

COBIT 5's 37 domains focus on how to run/manage capabilities across IT and helps maintain an acceptable risk level.

SOX Control Family	Corresponding COBIT 5 Practice Supported by Exabeam	Exabeam SOX Capabilities
Align, Plan, and Organize (APO)	• Manage the IT Management • Framework [APO01] • Manage Strategy [APO02] • Manage Human Resources [APO07] • Manage Service Agreements [APO09] • Manage Suppliers [APO10]	• Monitoring of security events, detection of compromised credentials • Ensuring effectiveness of security controls • Effective incident response • Enabling rapid investigation and reporting
Build, Acquire, and Implement (API)	• Manage Solutions Identification and Build [BAI03] • Manage Availability and Capacity [BAI04] • Manage Changes [BAI06] • Manage Change Acceptance and Transitioning [BAI07] • Manage Configuration [BAI10]	• Leveraging Risk Scores • Monitoring IT Operations and Change Control Processes
Deliver, Service, and Support (DSS)	• 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 • Effective Incident Response • Ensuring Effectiveness of Security Controls • Enabling Rapid Investigation and Reporting
Monitor, Evaluate, and Assess (MEA)	• Monitor, Evaluate and Assess Performance and Conformance [MEA01]	• Ensuring Effectiveness of Security Controls • Effective Incident Response • Enabling Rapid Investigation and Reporting

CONCLUSION

Along with SOX regulations comes a slew of requirements that Exabeam can help you meet. Our products are created with compliance in mind, and we deliver a purpose-built solution to help security teams of all sizes stay on top of SOX compliance. With Exabeam, security teams benefit from SOX-ready solutions while also having effective threat management capabilities.

To learn more about how Exabeam can help your organization adhere to SOX regulations, schedule a demo with us today!