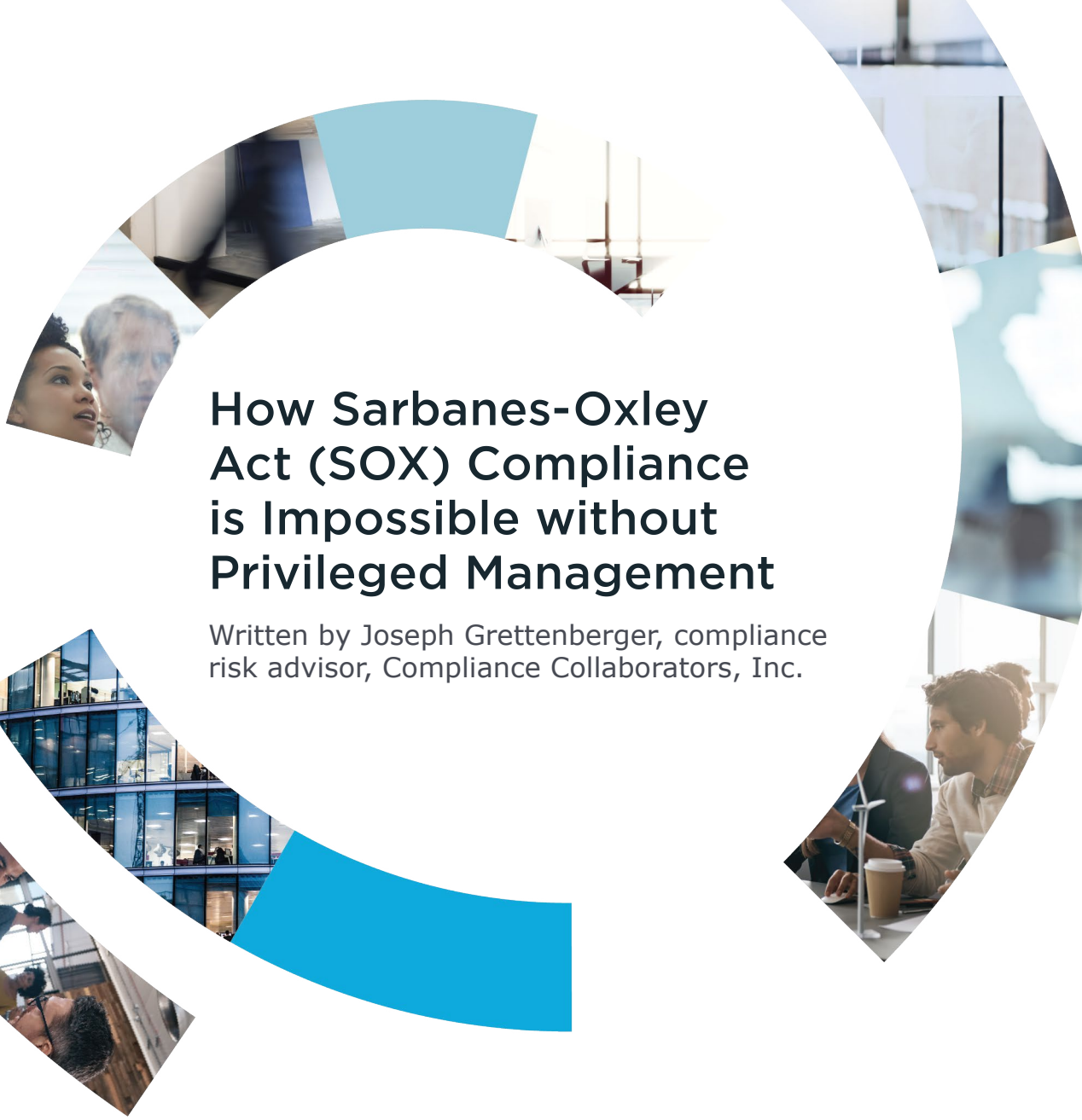
TECH BRIEF



How Sarbanes-Oxley Act (SOX) Compliance is Impossible without Privileged Management

Written by Joseph Grettenberger, compliance risk advisor, Compliance Collaborators, Inc.

Introduction

For many organizations, compliance with data security standards doesn't seem to be getting easier. IT security compliance efforts are forever competing with projects to address ever-pressing information security threats, operational vulnerabilities and daily business risks, and they often lose out in the battle for resources and funding.

However, the reality is that these areas do not have to compete. By implementing proven solutions that address multiple foundational controls, you can achieve and prove regulatory compliance while guarding against the risks that threaten everyday operations or even land organizations in the headlines. For example, a key component of regulatory compliance is implementing (and demonstrating that you have implemented) appropriate IT-related internal controls that minimize the risk of fraud and data breaches. Achieving and proving your compliance with such mandates requires you to mitigate the security risk of system users obtaining unauthorized access to sensitive data — and implementing these privileged management controls will also further your organization's broader security goals.

This paper addresses this area of IT security compliance from an auditor's perspective for the Sarbanes-Oxley Act (SOX). Although SOX represents only a portion of the total scope of compliance obligations faced by most organizations, it is a critical

piece of the compliance challenge, and the solutions recommended here for SOX compliance will help your organization achieve and prove compliance with other security mandates as well. For example, to learn more about how these solutions help with Payment Card Industry Data Security Standard (PCI DSS) compliance, please see the white paper, "Why PCI DSS Compliance is Impossible without Privileged Management."

Sarbanes-Oxley Act (SOX)

Establishing standards for corporate governance

The Sarbanes-Oxley Act, passed by the U.S. Congress on July 30, 2002, was enacted to combat corporate accounting fraud that came to light with the corporate scandals of 2001 and 2002. Ultimately, the intention of SOX was to renew public confidence in U.S. securities markets.

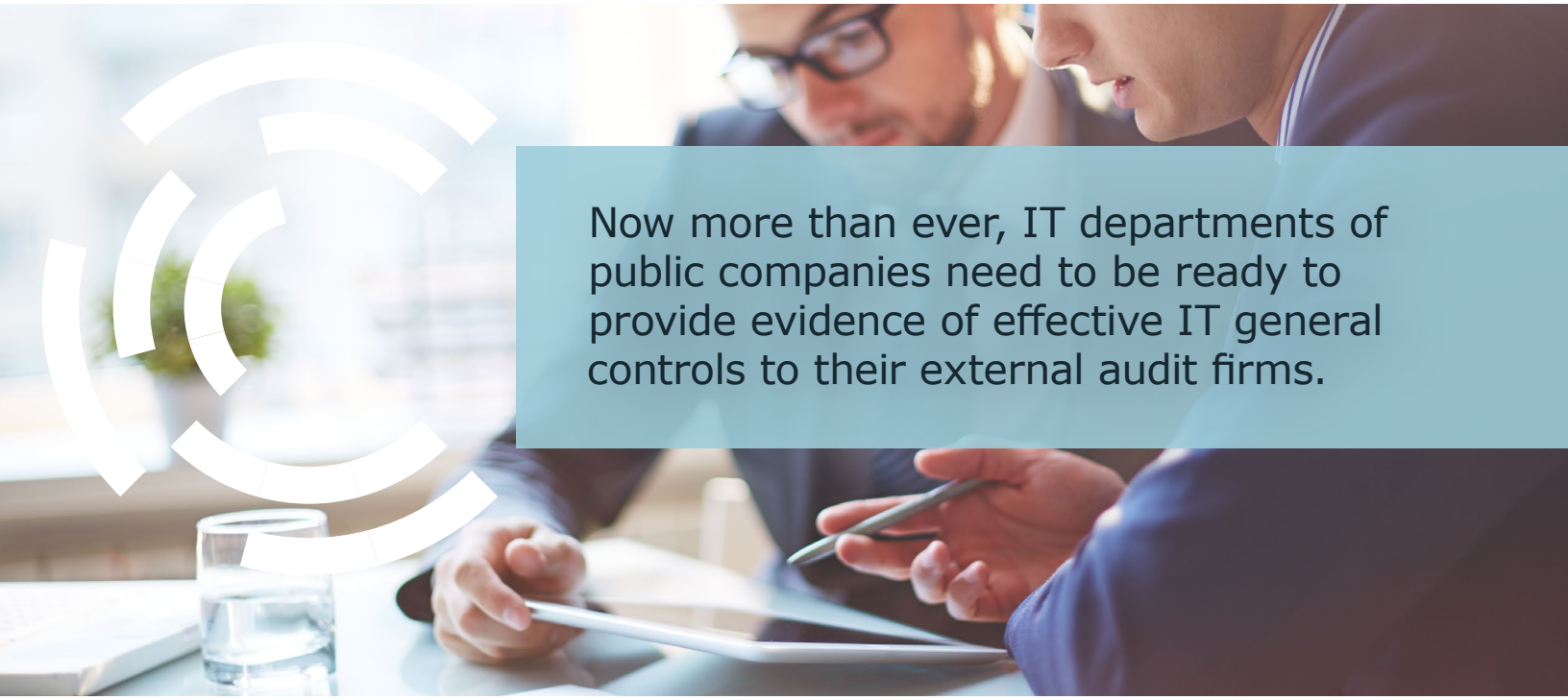
In particular, SOX advanced the standard for corporate governance by requiring that board-level audit committees, rather than CEOs or CFOs, "be directly responsible for the appointment, compensation, and oversight" of the external auditing of public companies, that no conflict of interest exist between audit committee members and accounting firms hired to perform such audits, and that the accounting firm have a direct line of independent reporting to such committees.[1] This requirement for a direct line of independent reporting to a company's board put responsibility on both the external auditor and the audit committee to review all potential sources of material misstatement of a company's financial statements, including any discovered significant deficiencies or material weaknesses that might prevent an auditor from rendering a favorable opinion.

New guidance for external auditors

Recently, however, the Public Company Accounting Oversight Board (PCAOB), which enforces SOX auditing standards, has warned public company accounting firms that certain traditional audit effort reduction practices will no longer be acceptable in Internal Control over Financial Reporting (ICFR) audits. Specifically, these firms can no longer provide audit opinions based on observations that rely on the work of others or on prior year audits without establishing a sufficient basis for using that work or otherwise providing current substantive evidence of having supervised, evaluated, tested or re-performed such work.[2] Instead, audit firms are now being asked to substantiate clean opinions with substantive evidence of internal control uniformity across the enterprise that indicate a level of

[1] *Sarbanes-Oxley Act, Section 301.*

[2] *PCAOB Staff Audit Practice Alert No. 11, pp. 12-13, 29-32.*



control design, implementation and operating precision sufficient to detect error that could cause material misstatement.

Protected information is stored and transmitted in a variety of systems across an organization's network.

In the early days of SOX, the SEC and PCAOB had very little guidance to provide the audit community regarding the shared responsibilities for evaluating an organization's IT control risk in the context of ICFR other than to point internal and external auditors to those technology controls that could be a "source of likely potential misstatements" in the financial statements. As financial audit practices matured, the PCAOB recognized the need for external auditors to intelligently assess the information technology controls involved in ICFR audits.

Two standards are of particular import here:

- **PCAOB Auditing Standard No. 5**, which states that "the auditor should assess … the extent of information technology ('IT') involvement in the period-end financial reporting process."
- **Auditing Standard No. 12**, which states, "The identification of risks and controls within IT is not a separate evaluation. Instead, it is an integral part of the approach used to identify significant accounts and disclosures and their relevant assertions and, when applicable, to select the controls to test, as well as to assess risk and allocate audit effort."

The impact on corporate IT

The trend towards using technology in virtually every step of the process of producing financial statements, combined with this pressure on audit firms to provide additional evidence, has in turn placed pressure on public companies to identify, collect and provide more evidence of effective IT general controls (ITGCs). Now more than ever, IT departments of public companies need to be ready to provide evidence of effective IT general controls to their external audit firms.

What does this entail? SOX ITGCs, which are implied in section 302 and 404 of the Act, include both basic and enterprise-wide IT security controls that require organizations to:

- **Reduce opportunities for financial data tampering** — One strategy is to enforce a disciplined process of authorizing privileged user roles and responsibilities around financial data not only within the application layer but also within its underlying technologies. This would include defining who is authorized to approve access to the infrastructure of financial systems, including network and server hardware, operating systems, log files, and databases of applications running financial transactions such as purchase orders.
- **Reduce opportunities for reporting period tampering** — For example, organizations can enforce least-privilege access control models at the operating system level of the financial data environment, audit all system time change events, and monitor activities of user accounts with access to system time clocks.
- **Monitor who had access to what financial information and when** — This could include monitoring activities of user accounts with access to servers that record, transmit or store activity on systems containing financial data.
- **Monitor automated transactions that affect financial data** — Examples include inventory movements and account reconciliations.
- **Monitor manual transactions** — This includes, for instance, post-closing journal entries.
- **Ensure ongoing effectiveness of controls** — For example, organizations should actively review all suspicious events occurring within their IT systems and provide their external

auditors the results of this process.

Risks that every organization should assess

While the text of the Sarbanes Oxley Act does not specifically mention internal controls for access to financial data, it's clear across all industries that an issuer's signing officers cannot assert that their company has an effective system of internal controls without ensuring properly controlled access to their financial data, via both financial applications and the underlying infrastructure. For privileged access to be properly controlled, at a minimum, all public companies must assess the following risks:

- Lack of separation of development and test environments from the live production environment, including but not limited to proper network segmentation and controls around changes in the production environment
- Unauthorized or unmonitored privileged access to financial data the company relies on or could potentially rely on when preparing its financial statements
- Unmonitored significant financial transactions, financial data updates and related system controls at the application, database, operating system, hypervisor, network device and hardware level (including connections from all possible accessing devices)
- The abuse of system accounts and privileged utility programs
- Unauthorized, unmonitored or uncontrolled modifications to source code
- The use of weak passwords, default passwords, static passwords, unencrypted stored or transmitted passwords, shared user accounts, non-named accounts, and aging accounts in all environments where financial data, authentication data or source code exists
- Persons granted multiple privileged access profiles (for example, roles) that produce a conflict of interest

One Identity privileged account management (PAM) solutions

The security features of primary applications are insufficient.

With all of the risks that can arise from poorly managed privileged access, it is not surprising that auditors today look for extensive controls related to privileged access management. But using the group permissions and role-based management features of primary applications (financials, payroll, ERP, POS, e-commerce and so on) to protect sensitive information is not enough to safeguard that information. ICFR auditors know that protected information is stored and transmitted in a variety of systems across an organization's network, including the support systems (such as file servers, mail servers, backup servers, development and test servers, and network devices) and underlying platforms (databases, operating systems, hypervisors and VM hosts) that make up the environment outside the organization's primary business applications. Therefore, those systems and platforms must also be included in the ICFR risk analysis and protected by appropriate controls.

> Organizations need to supplement application-based security features with privileged account access controls that protect the entire environment subject to compliance regulations.

Automating privileged account management and streamlining compliance

When auditors evaluate a financial statement control risk, such as monitoring user access to financial data and management override situations, PCAOB Auditing standard No. 5 points

them to consider the "degree to which the control relies on the effectiveness of other controls." For a proper controls reliance strategy, organizations need to supplement application-based security features with privileged account access controls that protect the entire environment subject to compliance regulations. And given the complexity of those regulations and the ever-changing threat landscape, organizations need as much automation as they can get.

One Identity privileged account management solutions automate many of the assurance safeguards required by today's IT security mandates while also providing foundational IT security measures.

One Identity privileged account management solutions automate many of the assurance safeguards required by today's IT security mandates while also providing foundational IT security measures. For example, the three One Identity PAM solutions highlighted in this paper address requirements for IT general controls in all five internal control components of SOX, as well as six of the 12 PCI DSS requirements, 12 of the 18 standards in HIPAA's Security Rule, and 28 of the 35 control objectives in ISO 27001, Annex A.

Specifically, One Identity PAM solutions enable organizations to:

- Substantially automate the enforcement of privileged access management, including requests, reviews, approvals, denials and revocations
- Quickly respond to management and audit inquiries with reports that demonstrate historical compliance with many information security policies and procedures
- Monitor and report on privileged activities, including those during sensitive time periods or outside the course of normal business operations
- Substantiate evidence of policy violations using a separate database of activity records, such as when personnel sanctions related to the security of information systems need to be applied

A more complete and effective solution

In short, One Identity privileged management solutions are designed to continuously manage routine and non-routine privileged access to the platforms and environments supporting critical applications and housing sensitive data — filling a critical security gap for traditionally weak ITGCs. The solutions equip organizations to adopt robust privileged account management and monitoring practices that augment and to some extent preempt standard user activity monitoring, malware and intrusion detection controls.

While not a replacement for network monitoring tools, when regularly used as part of an information system security program, One Identity PAM solutions can greatly reduce a host of unauthorized access and system changes — including unauthorized access to systems with sensitive data, unauthorized system configuration changes, unauthorized software downloads and more — thereby preventing numerous policy violations before they happen.

By enabling controlled use of administrative privileges, ensuring controlled access based on need-to-know, and providing detailed recordings of discrete activities performed in controlled environments, One Identity PAM solutions help organizations control privileged access to their production operating environments and ensure that critical access controls are applied to security architectures in all phases of the system development lifecycle.

The One Identity privileged account management solutions included in this paper are:

- Privileged Password Manager
- Privileged Session Manager
- Privilege Manager for Sudo

Privileged Password Manager

Privileged Password Manager automates, controls and secures the entire process of granting administrators the credentials necessary to perform their duties. It ensures that administrative or privileged access is granted according to established policy, with appropriate approvals; that all actions are fully audited and tracked; and that the password is changed immediately upon its return.

Privileged Password Manager also eliminates the security exposure posed by the embedded privileged passwords required for applications to talk to each other or to databases by replacing these hard-coded passwords with programmatic calls that dynamically retrieve the account credential. Privileged Password Manager is deployed on a secured, hardened appliance.

Privileged Session Manager

Privileged Session Manager enables authorized trusted personnel to issue privileged access for a specific period or session to administrators, remote vendors and high-risk users — with full recording and replay for auditing and compliance. It provides a single point of control from which trusted persons can authorize connections, limit access to specific resources, allow only certain commands to be run, view active connections, record all activity, alert if connections exceed pre-set time limits, and terminate connections.

This solution is also deployed on a secure, hardened appliance and, when combined with Privileged Password Manager, can completely hide the account password from the privileged user.

Privilege Manager for Sudo

Privilege Manager for Sudo enhances sudo with a central policy server that enables centralized management of sudo and the sudoers policy file, as well as centralized reporting on sudoers access rights and activities. It also performs keystroke logging, complete with search and playback capabilities, for in-depth auditing and compliance requirements. Privilege Manager for Sudo is part of the Privileged Access Suite for Unix.

Mapping SOX audit standards to One Identity PAM solutions

Exactly how will these One Identity PAM solutions help your organization achieve and prove compliance with specific SOX audit standards? The table below lists the IT-related requirements in the SOX auditing standards that public accounting firms use to audit U.S. public companies and maps them in two ways: to particular requirements in the SOX Act and to the specific capabilities of One Identity PAM solutions that will help you meet the audit standard. This table will help your organization review its related controls for possible gaps in compliance and find the right solutions to eliminate those gaps.

Audit standard	Requirement	SOX requirements addressed	How One Identity PAM solutions help
AS No. 5, Para 14	The auditor should evaluate … controls intended to address the risk of management override of other controls.	Partially addresses SOX 302(a)(2)	**Privileged Session Manager** and **Privileged Manager for Sudo** capture the activities of privileged sessions on systems with sensitive data, so you can implement a policy requiring all management overrides and other specified temporary privileged access be recorded and independently reviewed. Specifically, when the session recording function of these solutions is used consistently to record all management override situations, your company's auditors can review relevant activity records for abuse. For example, they can perform forensic analysis of suspect management overrides and potentially disguised management overrides, such as could occur during system maintenance periods or temporary, unplanned "break-fix" privileged access sessions.

Audit standard	Requirement	SOX requirements addressed	How One Identity PAM solutions help
AS No. 5, Para 46 & 47	The evidence necessary to persuade the auditor that the control is effective depends upon the risk associated with the control. … Factors that affect the risk associated with a control include … the effectiveness of entity-level controls, especially controls that monitor other controls.	Partially addresses SOX 302(a)(4) & (a)(5)	The centralized session recording and keystroke logging functions of **Privileged Session Manager** and **Privilege Manager for Sudo** provide detailed audit trails, which can be used for regular, periodic and forensic reviews of the activities of privileged IT users. To provide two examples, these solutions can be used to record and examine management's review of privileged account authorization history and anomalies discovered by continuous monitoring controls or manual system-monitoring controls, such as those related to or carried out by the IT security or IT systems and network operations groups. They can also be used to record and examine internal control assurance functions performed by internal auditing and management's review of those functions, including anomalies discovered by IT's continuous auditing controls. Both examples illustrate how organizations can capture evidence that provides insight into the effectiveness of entity-level monitoring controls, which are integral to organization's control reliance strategy (that is, the foundational ITGCs upon which other controls rely).
AS No. 5, Para 47	Factors that affect the risk associated with a control include … [t]he degree to which the control relies on the effectiveness of other controls (e.g., the control environment or information technology general controls).	Addresses SOX 302(a)(2), (a)(3), (a)(4) & (a)(5)	Many of the internal controls required for keeping risks of financial reporting misstatements to an acceptable level (such as those preserving the integrity of period-end reports) rely on the effectiveness of ITGCs. **Privileged Password Manager, Privileged Session Manager** and **Privilege Manager for Sudo** help preserve the integrity of financial data by reducing risks such as unauthorized privileged access from credential harvesting of static passwords and the spread of malware across the network.
AS No. 5, Para 47	An automated control would generally be expected to be lower risk if relevant information technology general controls are effective.	Addresses SOX 302(a)(2), (a)(3) & (a)(4)	**Privileged Password Manager, Privileged Session Manager** and **Privilege Manager for Sudo** can greatly increase the effectiveness of privileged account and password management, systems access management, controlled access to sensitive financial data, and granular privilege authorization, as well as demonstrate key elements in the level of precision of these controls.

Audit standard	Requirement	SOX requirements addressed	How One Identity PAM solutions help
AS No. 12, Para 21	Internal control over financial reporting can be described as consisting of the control environment, the company's risk assessment process, information and communication, control activities, and monitoring of controls.	Addresses SOX 302(a)(2), (a)(3), (a)(4), (a)(5), (a)(6) & 404(a)(2)	**Privileged Password Manager, Privileged Session Manager** and **Privilege Manager for Sudo** are designed to control and manage access and edit privileges on systems with sensitive data. When deployed enterprise-wide, these tools serve as foundational ITGCs to help prevent unauthorized access, monitor all privileged access, and capture file and folder permission changes in recorded sessions for later review. Examples of where the recording capabilities of these tools come in useful include reviewing privileged access to: • Sensitive files • Unauthorized activities • Changes to significant accounts or databases
AS No. 12, Para 28(d)	The auditor should obtain an understanding of … [h]ow the information system captures events and conditions, other than transactions, that are significant to the financial statements (e.g., including conditions affecting the recoverability of assets).	Addresses SOX 302(a)(2), (a)(3), (a)(5)(B) & 404(a)(2)	Privileged users who access any system that contains data used for financial statements could make significant changes that could affect the outcome of the company's financial statements. **Privileged Session Manager** can record and play back all actions taken by users with privileged access. This ensures that all potentially significant events and conditions made by such users are captured in your organization's information systems. This includes significant events outside the automated controls of the financials, such as low-level (raw) data changes to material attributes of a significant account or its authorization data, or metadata changes occurring outside financial transactions. Other privileged sessions to consider recording include deletions of archives and backups, material changes to contracts affecting significant accounts (contract length, payment terms and so on) and changes to calculations in an insurance company's premiums.
AS No. 12, Para 35(i)	The auditor should obtain an understanding of … the major types of activities that the company uses to monitor the effectiveness of its internal control over financial reporting.	Addresses SOX 302(a)(4)(C), (a)(4)(D) & 404(a)(2)	**Privileged Password Manager, Privileged Session Manager** and **Privilege Manager for Sudo** can monitor privileged IT system activities that can affect the automated controls that your company must address to determine the effectiveness of its internal controls over financial reporting.

Audit standard	Requirement	SOX requirements addressed	How One Identity PAM solutions help
AS No. 12, Para 35(ii)	The auditor should obtain an understanding of … how the company initiates corrective actions related to its controls.	Partially addresses SOX 302(a)(5) & (a)(6)	All corrective actions related to an organization's internal controls should be assigned and authorized by a person with proper authority. **Privileged Password Manager, Privileged Session Manager** and **Privilege Manager for Sudo** ensure that corrective actions initiated to remediate ineffective ITGCs and application controls are properly authorized and monitored in real time or recorded for later review.
AS No. 12, Para 36	The auditor should obtain an understanding of … the source of the information used in the monitoring activities.	Partially addresses SOX 302(a)(2), 302(a)(4)(D), 404(a)(2) & 404(b)	The privileged session recordings of **Privileged Session Manager** and recorded keystrokes of privileged account activities captured by **Privilege Manager for Sudo** are sourced from their respective operating platforms and stored in a central history vault.
AS No. 12, Section B4, example #2	The auditor should obtain an understanding of … unauthorized access to data that might result in destruction of data or improper changes to data.	Partially addresses SOX 302(a)(2) & 302(a)(5)(B)	**Privileged Password Manager, Privileged Session Manager** and **Privilege Manager for Sudo** can virtually eliminate unauthorized privileged access to systems that contain sensitive data. They provide a secure, centralized privileged access authorization workflow that ensures permissions to sensitive systems are formally requested, reviewed for approval, monitored if needed, and terminated once the window of approval is expired, regardless of the platform.
AS No. 12, Section B4, example #3	The auditor should obtain an understanding of … the possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties.	Partially addresses SOX 302(a)(2) & (a)(3)	**Privileged Session Manager** and **Privilege Manager for Sudo** support least privilege access policies by enabling organizations to easily manage and enforce minimum necessary access models for systems, databases and privileged sessions. Moreover, these solutions enable you to demonstrate both historical and current access privileges by providing a management console and a variety of reports that enable authorized persons to review current access rights, as well as what changes were made to which systems, programs and files; who made those changes; and when the changes were made.
AS No. 12, Section B4, example #4	The auditor should obtain an understanding of … [u]nauthorized changes to data in master files.	Partially addresses SOX 302(a)(2)	In systems containing master files where activities are not logged by application controls but where authorized approvals for privileged access to master files is required, **Privileged Session Manager** provides detailed session recordings and **Privilege Manager for Sudo** provides complete keystroke records that can be used for forensic analysis discovery of who may have made unauthorized changes to data in master files.

Audit standard	Requirement	SOX requirements addressed	How One Identity PAM solutions help
AS No. 12, Section B4, example #5	The auditor should obtain an understanding of … [u]nauthorized changes to systems or programs.	Partially addresses SOX 302(a)(2) & (a)(3)	Change management is a foundational control for keeping unauthorized changes out of your organization's production operating environment. **Privileged Password Manager, Privileged Session Manager** and **Privilege Manager for Sudo** can manage and enforce a change approval process in both development and production environments. These solutions also employ randomized passwords, which further reduces the likelihood of unauthorized changes to systems or programs. When combined with appropriate system account authorization controls, randomized passwords also help organizations control activities in which malicious software is known to infect a network, such as new software downloads, automated software updates and unauthorized software installs.
AS No. 12, Section B4, example #9	The auditor should obtain an understanding of … potential loss of data.	Partially addresses SOX 302(a)(5) & (a)(6)	Data loss can pertain to data availability (such as deletion), confidentiality (such as exfiltration) or integrity (such as tampering). **Privileged Password Manager, Privileged Session Manager** and **Privilege Manager for Sudo** minimize the risk of data exfiltration by auto-generating randomized passwords, thus greatly reducing the likelihood of pass-the-hash, credential harvesting and similar exploits. In addition, **Privileged Session Manager** can record everything a user does within a privileged access session, and **Privilege Manager for Sudo** can log all keystrokes. While these features do not prevent data deletion or tampering, if a privileged user deletes, exports, downloads or tampers with data, the action will be recorded and logged, enabling forensic analysis of potential data loss.
AS No. 15, Para 10	When using information produced by the company as audit evidence, the auditor should … test the controls over the accuracy and completeness of that information.	Addresses SOX 302(a) & 404(b)	To ensure a complete and accurate history of privileged users' rights and access, **Privileged Password Manager, Privileged Session Manager** and **Privilege Manager for Sudo** store all relevant information in a centralized password safe that is secured using full disk encryption. This data includes all recorded sessions, keystrokes, and data associated with workflow history — including requests, reviews, approvals and passwords. This data is available both in the tool and through customizable reports, enabling quick and effective response to audit inquiries.

Privileged Password Manager, Privileged Session Manager and Privilege Manager for Sudo can enable you to efficiently manage privileged access to sensitive systems and financial data within the wider business data environment.

Conclusion

The user access controls included in business financials and financially related applications provide only a portion of the security you need to achieve, maintain and demonstrate SOX ICFR compliance. To pass ICFR audits, you also need to manage privileged access to your organization's entire business data environment — including the systems and underlying platforms that store or protect the integrity of financial data — throughout the entire development lifecycle.

Privileged Password Manager, Privileged Session Manager and Privilege Manager for Sudo can enable you to manage privileged access to sensitive systems and financial data within the wider business data environment, and they deliver the automation you need to do so effectively and efficiently. For more information, please visit oneidentity.com/privileged-management.

About the author

Joe Grettenberger has over 25 years of experience as an IT assurance professional, including eight years of technology auditing experience in both the public and private sectors. He is certified as an information systems auditor (CISA) and as is compliance & ethics professional (CCEP), and has served clients for over six years as an IT governance and risk management consultant covering a wide range of IT assurance issues within the regulatory, legal and industry compliance space.

Grettenberger has held IT audit, assurance and advisory positions at a number of organizations, including Modern Compliance Solutions, Quest Software, Vintela, Center 7, Franklin Covey and SAIC. He started his own consulting practice in 2008. He was a recent participant in the Internet Security Alliance initiative to promote cross-industry IT security standards, and he has also participated in several other standard-setting best practice initiatives, including serving on the SunTone Architecture Council and chairing the MSP Association's Best Practice Committee. www.compliancecollaborators.com

For More Information

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (**www.oneidentity.com**) for regional and international office information.

ONE IDENTITY