KEEPER
Cybersecurity Starts Here

Keeper Supports Sarbanes-Oxley (SOX) Compliance

DATASHEET

SOX Compliance

The Sarbanes-Oxley Act (SOX), which was enacted into U.S. federal law in 2002, established a set of anti-fraud controls that apply to public companies and companies that are considering a potential initial public offering (IPO). SOX or Sarbox also applies to wholly-owned subsidiaries and foreign companies that are publicly traded and do business in the United States, as well as accounting firms that perform SOX compliance audits.

The goals of SOX are to ensure the accuracy and transparency of corporate disclosures and to protect enterprise shareholders and the general public from accounting errors and fraudulent practices.

Automation is Crucial to SOX Compliance in the Remote Work Era

The COVID-19 pandemic touched off a worldwide increase in cyberattacks that INTERPOL called "alarming." Cybercriminals are taking advantage of increased security vulnerabilities as organizations rapidly deploy technologies to enable large numbers of remote workers.

In this high-risk environment, SOX compliance professionals are seeking to make changes to their existing compliance technologies and processes.

SOX audits require organizations to provide voluminous documentation providing that they have established internal controls spanning five key areas, and that these controls are working effectively:

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

While SOX audit reports are produced annually, organizations must prove that their controls are operating continuously, year-round. This means that audit-related activities take place throughout the year, placing additional burdens on already-overworked IT staff. It is crucial that organizations automate as many SOX compliance processes as possible.

Using Keeper to Support SOX Compliance

The protection of credentials and access to financial systems is essential for organizations to comply with SOX financial reporting and disclosure requirements. Every user within an enterprise network is a potential risk factor, making it critical to ensure risk mitigation and data protection for every employee, subcontractor, and vendor, on every device that accesses the organizational network.

Keeper simplifies SOX compliance monitoring and reporting by giving IT administrators full visibility and control over employee password usage and role-based systems access throughout their data environments, with customizable audit logs and event reporting. Keeper supports robust internal controls through delegated administration, enforcement policies, event tracking, monitoring, and reporting.

IT Admin Insight

Every employee is provided with a secure digital vault. A security dashboard in the Admin Console provides an overview of weak passwords, password reuse, and 2FA enforcement, along with role-based-access-controls (RBAC) to enforce least privilege policies. Administration may be delegated according to department or by team leader, and folders and records can be securely shared and revoked. If an administrator or employee leaves the company, their vault can be automatically locked and securely transferred. Access logs to Keeper vaults can be audited for compliance or forensics.

SOX Audit Reporting

The Keeper Commander SDK enables administrators and authorized end-users to run reports relevant to meeting SOX compliance requirements, including:

Shared Access Report - The share-report command provides a breakdown of which users within the organization have access to records within the vault. This report is generated based on the specific user currently logged into Commander.

Keeper Security's Advanced Reporting & Alerts module (ARAM) empowers IT administrators to monitor any size user population; receive focused, summary trend data and real-time notifications of risky or unusual behaviors; and run customized reports. For example, the audit-report command provides detailed event-based reporting at the user, record, or overall system level.

Keeper enables administrators to easily define custom SOX reports that include detailed events related to sharing information including who the information has been shared with and any permission changes related to access. For more information on ARAM, please reference the **Keeper ARAM datasheet.**

Email Auto-Provisioning

Easily and quickly provision Keeper vaults to tens or thousands of users, with a domain match on email addresses. With minimum administration, large-scale deployment can be accomplished using an existing email channel or portal.

Flexible Provisioning

Keeper supports the ability to seamlessly provision users and teams from Microsoft Azure AD or other identity platforms using the SCIM protocol. Keeper also supports API-based, command line provisioning through the use of Keeper Commander SDK. The Keeper Commander SDK is open-source Python code that is available for download from Keeper's Github repository.

Secure File Storage

In addition to securing employee passwords, Keeper helps companies prevent data loss by allowing them to store sensitive files, documents, digital certificates, private keys, photos, and videos in a highly secure, encrypted digital vault. Employees can securely share files with colleagues with confidence, knowing that only the intended recipients can access the shared files.

Keeper uses PBKDF2 to derive authentication keys based on the user's Master Password, then generates individual record-level AES-256 encryption keys locally on the device to encrypt each stored file. Keeper's cloud only holds the encrypted ciphertext of each file. Sharing between users is performed using PKI to ensure that only the recipient of a shared file can decrypt it. Keeper's zero-knowledge encryption methods ensure that only the user can access and decrypt their stored files.

Defense Against Third-Party Vendor Breaches

Even if your password security is solid, your firm could be compromised through one of your vendors. With remote workforces having rapidly expanded, cybercriminals are taking advantage of the myriad of SaaS solutions that businesses are deploying to enable their remote workforces. Keeper supports granular controls that allow an administrator to restrict third party vendor access to information and critical systems, while requiring strict access control and account monitoring. Custom alerts and reports can be configured to monitor, track, and notify administrators of any risky behavior. Administrators can then take action which may include locking these third party vendor accounts.

Keeper BreachWatch™ for business protects your organization, including third-party vendor accounts, against breaches caused by compromised credentials. BreachWatch for business doesn't depend on public breach notifications. It scans Dark Web forums and notifies organizations in real-time if any employee passwords have been compromised. This allows IT administrators to force password resets right away, minimizing the risk of cybercriminals using them to breach company systems.

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the market-leading, top-rated cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM). Learn more at **https://keepersecurity.com/enterprise.html.**