ConductorOne

# SOX Access Controls, Separation of Duties, and Best Practices


The Sarbanes-Oxley Act, commonly known as SOX, is a US federal law that requires corporations to perform specific recordkeeping and reporting practices. The law was created in 2002 in response to several corporate and accounting scandals in large companies like Enron, Tyco International, and WorldCom. Cybersecurity requirements for financial systems were brought further into the spotlight with the Dodd-Frank Act in 2010, which imposed requirements to report significant security events and weaknesses of publicly traded companies.

SOX protects investors by improving the accuracy and trustworthiness of corporate disclosures for publicly traded companies. According to the law, organizations' senior management must disclose financial status accurately and ensure that the act's technical and nontechnical requirements are met and audited by independent third parties. Failure to adhere to the law can lead to fines or even imprisonment of the chief executive officer (CEO) and chief financial officer (CFO).
The act's primary goals are as follows:

- **Improve financial transparency:** SOX requires corporations to make accurate and thorough financial disclosures and ensure that financial statements truly reflect the condition of a company. Corporations must also make real-time disclosures if a material change to their financial condition occurs.
- **Prevent accounting fraud:** SOX introduced measures to ensure that auditors are independent of the companies they audit and that individual responsibility lies with corporate executives. It also established the Public Company Accounting Oversight Board (PCAOB) to directly oversee the activities of the auditing profession in the US and through cooperative agreements abroad. It's not directly part of the US government, but it operates under the oversight of the US Securities and Exchange Commission (SEC).
- **Protect whistleblowers:** SOX has mechanisms to protect whistleblowers who report violations of security laws or fraud, including confidential reporting and antiretaliation provisions.
- **Hold executives accountable:** Under SOX, top management must individually certify the accuracy of financial information. It criminalizes fraudulent activities of CEOs and CFOs who certify false financial reports.

This article explores the intricacies of SOX access controls and introduces some methods and best practices to simplify compliance and overcome challenges.

## Understanding SOX Access Controls and the Separation of Duties

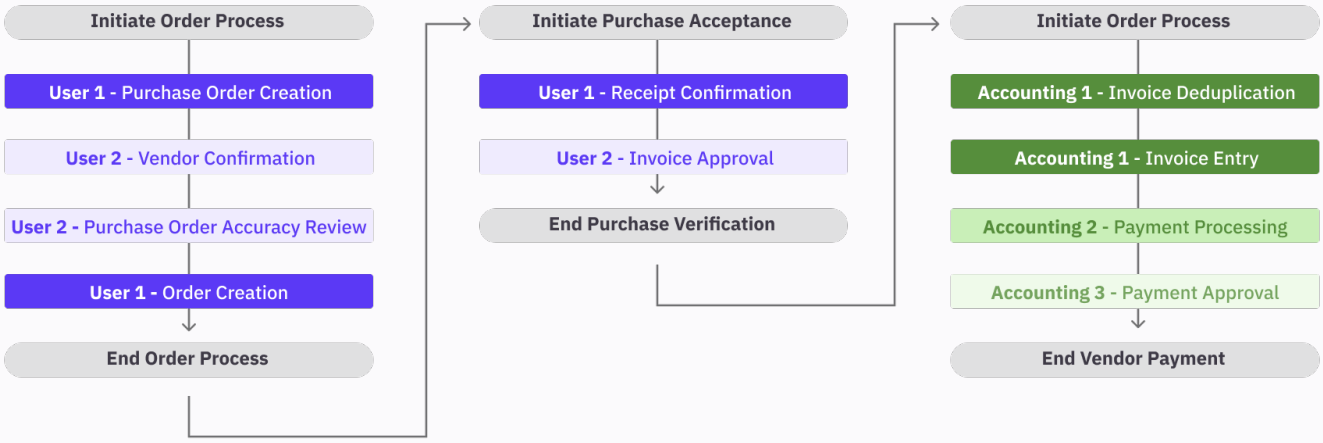
User access control is a key component of SOX.
Access control essentially involves organizations controlling permissions in their financial systems and who can access and manipulate data related to financial transactions.
While access control is usually associated with passwords, it's more than that. It's about using strong authentication techniques, routinely checking accounts with access to financial data, and keeping records of access activities.

Access controls must extend to a much wider area than just accounting and financial reporting software. It includes a broad range of technologies to manage, process, and

record financial transactions and data, from production billing systems that generate invoices and track revenue to contract management systems that record agreements and obligations. The scope of SOX compliance extends to any system that serves as an input to accounting records and financial statements. A financial system also involves databases, spreadsheets, and even manual processes that contribute to an organization's financial reporting.

Along with access control, organizations are responsible for imposing separation of duties (SOD). This principle ensures that no individual person can bypass a financial transaction's checks and balance controls (for example, a person cannot issue an invoice and approve it for payment). SOD reduces the chances for mistakes and opportunities for dishonesty in financial tracking and reporting periods. SOD requires clear definitions for roles, measures to avoid role conflict, and regular checks of user accounts. Access control is not the same as or a substitute for SOD. Instead, it is an enforcement mechanism—accounts should have the minimum access needed for their owners to perform their responsibilities, and accurate logging and monitoring are used to spot irregularities surrounding these transactions.

For instance, this diagram shows three related processes: ordering, purchase reconciliation, and payment:




Anywhere that there could be the creation and approval of a financial transaction, those duties are separated. Purchasing and order processing are key areas for financial integrity in almost any organization. Although the preceding diagram shows four roles—two for purchase creation and two for payment—this is not a required arrangement. Any responsibility assignment that separates creation, verification, and payment would be sufficient.

## Making SOX Compliance Simple and Efficient

Ensuring your organization is SOX-ready is notoriously difficult, especially for organizations with a small information security staff. There are multiple types of work to be performed, involving IT staff, financial staff, and human resources. All these are crucial to the implementation of a solid program.

## Streamlining SOX Compliance Processes

The protection of financial data starts with understanding how to handle it. The input, transactions, and output of financial processes are relevant points for control, but the controls must be assigned to—and tailored for—the processes:

1. **Identify and document key processes:** The organization must identify how financial data is handled and who is the owner of those processes. The owner is accountable for detailing where data enters the process, how data is handled and stored, and what occurs after data is processed. This process must be documented, and it cannot be changed without the review and approval of its owner.
2. **Map controls to processes and identify control owners:** After key processes are documented, internal controls are applied to the process. The owner should work with the designated SOX compliance owners to document and apply protections. When the satisfactory set of controls is documented, the owners of these controls are also chosen and documented. This allows monitoring and compliance reporting to the role who holds responsibility. Wherever the process changes, controls must be reviewed and potentially retired or added in order to accommodate the new processes.
3. **Establish a framework for monitoring and testing controls:** The assignment of controls does not guarantee that controls are configured and applied correctly. When controls have been chosen and implemented, they must be tested to ensure adequate functionality. Afterward, the controls must be monitored for continued efficacy. Without ongoing monitoring and testing, a control owner will not realize that the protections have stopped functioning as they should. Control owners should determine the important metrics for control behavior and the time frame for monitoring, reporting, and testing. These decisions should be based on the relative risk or importance of both the financial process and the implemented control.

## Automating SOX Compliance

One of the easiest ways to simplify SOX compliance is to use specific compliance technology. Tools for control testing, automated workflows, and software solutions for documenting compliance activities can create an efficient set of processes with built-in monitoring and assurance. The following are some examples of SOX compliance that can be enhanced with automation, including the appropriate automation and the SOX requirement that is fulfilled:

1. **Leverage technology and tools for control testing and monitoring:** Automation plays a pivotal role in control testing and monitoring by consistently evaluating controls to ensure they're functioning as intended. This regular testing reduces the need for manual checks, ensuring timely detection and correction of discrepancies.
    - **Example:** An automated system checks monthly sales data against inventory reductions, flagging discrepancies.
    - **SOX requirement (Section 404.a):** Ensuring accurate financial reporting and internal control over financial reporting.
2. **Implement workflow automation and approval processes:** Workflow automation streamlines various processes, from initiation to sign-off. By automating these workflows, companies ensure that tasks follow a consistent, documented path, reducing the risk of human errors.
    - **Example:** An employee's expense report is automatically routed for approval and payment.
    - **SOX requirement (Section 302.a):** Documentation and verification of transactions and processes.
3. **Utilize software solutions for documenting and tracking compliance activities:** Accurate and timely reporting is a SOX mandate. Automation aids in compiling and generating compliance reports on activities such as invoice approvals, system updates, data access records, and compliance training metrics.
    - **Example:** A system compiles financial data access and exception records into a quarterly compliance report.
    - **SOX requirement (Section 401.a):** Timely and accurate reporting of financial statements.

4. **Implement automation for data access control changes:** Data access controls are a cornerstone of data integrity, and most data access is linked to user accounts. Automated user account provisioning, deprovisioning, and permissions changes remove the potential for human errors or undesirable delays in account management.
    - **Example:** An employee changes roles from financial database administrator to a different project. Their permissions for the financial databases are removed when their role changes in the human resources system.
    - **SOX requirement (Section 404):** Internal control structures are required to protect financial data.

## Optimizing SOX Compliance

Regular risk assessments, continuous monitoring of control deficiencies, and implementation of remediation plans based on findings can significantly optimize the compliance process. This proactive approach continually aligns the organization's compliance posture with current risks and regulatory requirements. Section 404 of the Sarbanes-Oxley Act emphasizes the importance of management's responsibility not only to create but to maintain an "adequate" internal control structure. Furthermore, it mandates an assessment, conducted by the management, of the ongoing effectiveness of these controls. Any identified shortcomings in these controls must be transparently reported. The use of automated compliance monitoring and external auditors plays a crucial role in this adherence program. Maintaining a vigilant approach is the only way to ensure accuracy and monitor financial reporting.

# SOX Compliance Best Practices

Considering the long and specific list of requirements—and the heavy penalties for failure—enterprises need to understand the most efficient and surest methods to align with SOX. The best practices for SOX are not specific technical security implementations. Instead, they are components that provide shape, education, and accountability to guide personnel in the adoption of compliance.

## Access Controls for SOX Compliance

Access controls are an indispensable best practice for SOX compliance. They encompass various aspects of SOX, all tied to managing and monitoring access to a company's financial systems and data:

- **Principle of least privilege:** this involves restricting user and service accounts to access only what is necessary for their specific job roles, preventing unnecessary access even for authorized personnel.
- **SoD:** As mentioned, SoD is a specific requirement of SOX, and it's also best practice that helps establish checks and balances within the organization to prevent any single individual from having unilateral control over critical financial transactions.
- **Time-based restrictions:** These limit operational hours for system access, which minimizes the window for unauthorized activity.
- **Remote access controls:** These ensure secure channels for accessing systems outside of the controlled network, augmented with robust authentication protocols.

These controls are part of any complete security plan, but they are especially important for any organization that needs to protect financial information.

## Implementing a Robust Control Framework

A robust control framework actively streamlines the identification, assessment, and management of risks. Two popular options are the Control Objectives for Information and Related Technologies (COBIT) and the Committee of Sponsoring Organizations (COSO) Internal Control - Integrated Framework.

Both the COSO and COBIT frameworks deliver comprehensive guidelines, enhancing the efficacy of internal controls. Although not explicitly required for SOX compliance, the industry holds COSO and COBIT in high regard. These frameworks align businesses with industry benchmarks and best practices. By integrating COSO or COBIT standards, organizations elevate the reliability of their financial processing systems. Moreover, this alignment reinforces trust among external stakeholders, such as investors and regulators, underscoring the organization's dedication to solid financial controls.

## Establishing a Culture of Compliance and Accountability

Compliance with SOX is a baseline for the organization. While the ultimate accountability lies with the CEO and CFO, those executives rarely control the daily operations that produce financial reporting. Leaders must champion a culture of compliance and accountability, where adherence to SOX requirements is accepted as a shared responsibility between financial and IT personnel. Responsible teams and personnel within the organization must document changes, exceptions, and irregularities, reporting them as they occur. Risk is sometimes unavoidable, and circumstances may require acceptance of noncompliant activities. In those cases, an individual who is accountable for the risk must determine if the organization can justify the noncompliance.

The leadership of the organization must regularly communicate the status of compliance and, if necessary, expectations for changes needed to improve. This reinforcement of compliance mandates and support for compliance helps employees accept their roles in maintaining financial integrity.

## Conducting Regular Training and Awareness Programs

Education is a fundamental aspect of SOX compliance. All employees, from senior management to entry-level staff, must be informed about the significance of SOX and its implications. Specific departments, such as finance and recordkeeping, may require in-depth training due to their direct involvement with financial transactions and documentation. Individuals with legal responsibilities must be made aware of their accountability and any restrictions and requirements to which they are subject.

To ensure comprehensive knowledge across the organization, companies should organize structured training sessions and workshops. Additionally, providing accessible educational resources can offer employees a consistent reference point for regulation and the internal structures that support it. Awareness programs are available from multiple accessible vendors, including Udemy, and the executives who arrange training should be certain to differentiate those who need general awareness and those who need training on specific compliance responsibilities.

### Engaging Internal and External Stakeholders in the Compliance Process

SOX compliance is a collaborative effort that involves both internal and external stakeholders. The list of stakeholders should account for all teams involved in relevant activities. For instance, safeguards to prevent data tampering, as outlined in Section 302.2, require IT and finance teams to work together to implement systems that track user logins and detect unauthorized access attempts. Similarly, establishing verifiable controls to track data access, as mentioned in Section 302.4.B, requires collaboration between IT and operations to ensure that data collection from various sources is consistent and secure.

Internal stakeholders have an obvious interest in the success of SOX compliance activities. External stakeholders, too, should be ready to thoroughly engage so that the process runs smoothly. Collaboration with external auditors is also crucial, especially when disclosing security safeguards and breaches, as highlighted in Sections 404.A.1.1 and 404.A.2. External independent auditors provide an objective assessment of the company's compliance measures. Working with regulators and consultants offers a broader perspective, ensuring that the company's compliance measures are aligned with updated industry best practices as well as less volatile regulatory standards.

## Overcoming Challenges of Access Management for Sarbanes Oxley Compliance

Access control is a challenge for any organization. Operational and structural changes, personnel changes, and role adjustments all require constant access permissions updates. These necessary updates, coupled with an increasing volume of systems, applications, and data repositories, mean that access requirements are constantly shifting. Role-specific permissions add further complexity within each system.

### Access Control and Automation

Continuous review and maintenance of access control is integral to the effectiveness of internal controls over financial reporting. Regularly scheduled reviews serve as a proactive measure to maintain ongoing compliance. Access reviews also fulfill SOX's emphasis on accountability and traceability because it ensures the availability of auditable data. Without regular reviews, the accountable leadership cannot be certain that their systems continue to provide a trail of access permissions documentation. Removal of access information and account data is a common behavior for malicious intruders or anyone trying to hide their activities.

Automation for access reviews is not mandatory under SOX, but it offers advantages over manual reviews. Automation provides consistency, which eases the burden of scheduling and oversight for ongoing assessment. Automation also streamlines the compliance process and provides an automatic, auditable trail that can be invaluable during internal or external audits. The efficiency of automated access reviews allows leadership to focus resources on other SOX requirements that they can't cover with technical controls.

Real-time monitoring provides immediate, up-to-date records for all access-related activities. It is particularly relevant to the SOX requirements for tracking and reviewing access to financial systems. Real-time monitoring allows you to maintain a comprehensive audit trail of all access changes and gives the financial system owners an immediate view into activities that may raise concerns. In the case of suspicious or unauthorized activities, this capability helps minimize potential damage by allowing a step-by-step and immediate understanding of the changes that have occurred.

## Separation of Duties through Automation

SoD requirements add to the burden of access management and tracking. Whenever a new role or access profile is created to interact with financial data, you must compare that profile's access against other roles. Otherwise, you may accidentally create a role with a combination of permissions that breaches SoD – for example, allowing an employee to initiate and approve the same transaction. Automation can also provide a solution here. Revocation of access is a key control to ensure that authority is limited, even when a worker changes roles. Permissions and access changes linked to roles can be automated, ensuring that no one receives a too-permissive portfolio of abilities in financial systems.

## Improved Security through Least Privilege and Just-in-Time Access

Just-in-time (JIT) access and least privilege can further reduce the risk of fraudulent or inappropriate activity in financial systems. JIT allows temporary elevation of access permissions, often subject to multi-layered approval chains. This ensures that no individual has ongoing and potentially unsupervised privileges within critical financial systems. While JIT access solves many issues with unrestricted administrative access to information systems, it's beneficial in the context of SOX, where it helps mitigate the risk of fraudulent activities. JIT works well in scenarios that require immediate, short-term access since it eliminates the need for permissions that are only occasionally used. Additionally, as mentioned, the principle of least privilege mandates that users are granted only the minimum level of access necessary to perform their roles. By maintaining minimal access rights and removing unused or unnecessary permissions, organizations can use JIT to further align with the least privilege principles for SOX compliance.

# Conclusion

Managing SOX compliance demands scrutiny, forward-thinking strategies, and continuous improvement. This article sheds light on the core principles of SOX, offers approaches for efficient compliance, and highlights best practices for effective execution. For organizations seeking modern identity security solutions, ConductorOne delivers a range of tools tailored to boost SOX compliance and overall security measures. The platform focuses on identity security and governance, making sure that only the right individuals have access to sensitive information and systems. Their just-in-time provisioning ensures timely access to vital infrastructure, granting permissions only when necessary and revoking them afterward, and their automated access reviews eliminate the hassle of manually checking user permissions.