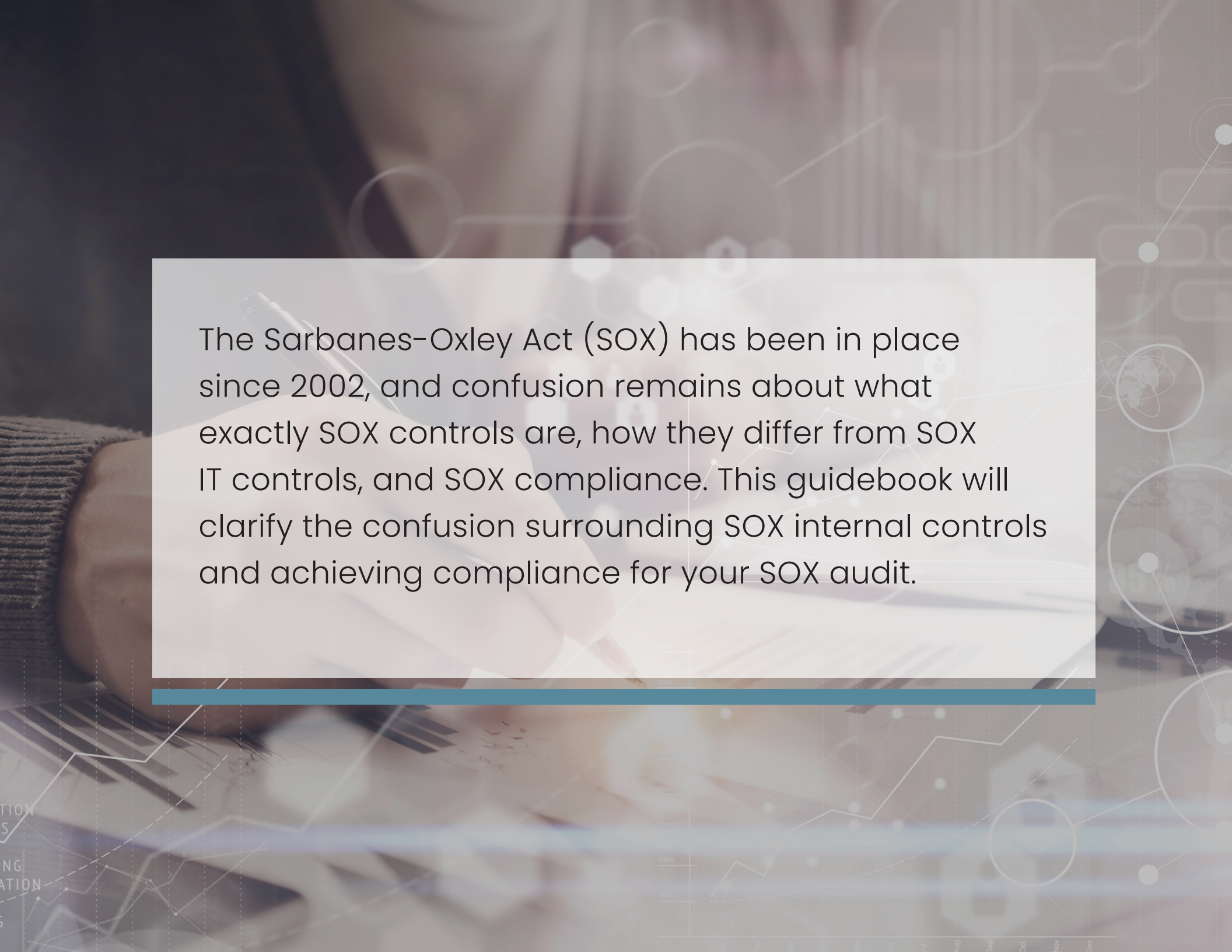




Guidebook for SOX internal controls compliance





The Sarbanes-Oxley Act (SOX) has been in place since 2002, and confusion remains about what exactly SOX controls are, how they differ from SOX IT controls, and SOX compliance. This guidebook will clarify the confusion surrounding SOX internal controls and achieving compliance for your SOX audit.

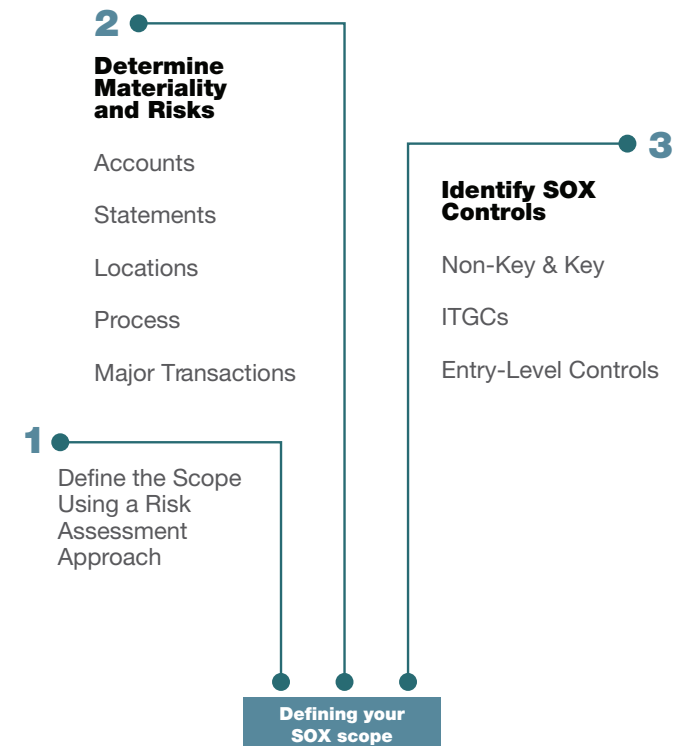
What are SOX controls?

SOX requires public companies to have [internal controls](#) over processes that impact financial reporting. These internal controls aim to ensure accurate and reliable financial reporting. However, there is confusion surrounding where SOX controls begin and where business process controls take over.

The overarching goal of SOX is to ensure the accuracy of financial reporting, which depends on business process controls and IT controls. Business process controls ensure the accuracy of the data that feeds into financial reporting systems. And IT general controls (ITGCs) and application controls secure the accuracy and completeness of the systems that store the data used in financial reporting.

Most of the confusion surrounding SOX controls is in the open-ended guidance regarding the type and number of controls required. SOX does not explicitly lay out the number of controls required. However, there are common types of controls for financial systems, such as system access, segregation of duties, change management, and data backup. The challenge is designing controls specifically for the systems on your network that meet your control objectives.

ACCOUNTS, STATEMENTS, LOCATIONS, PROCESSES, AND MAJOR TRANSACTIONS
ACCURACY OF THE DATA THAT FEEDS INTO FINANCIAL REPORTING
ENSURE THE SYSTEMS ARE ACCURATE, COMPLETE, AND FREE FROM ERROR
CAPTURE FINANCIAL DATA THAT FEEDS INTO YOUR FINANCIAL REPORTING



What are SOX key controls, and how to identify them?

The term “key control” is not officially included in PCAOB audit standards. However, PCAOB AS5 states that the higher the risk of material weakness in internal control over financial reporting (**ICFR**), the more attention audit will give to that risk.

Also, the risk that a company’s ICFRs will fail to prevent or detect fraud is typically higher than the risk of failure to prevent or detect errors. Again, auditors will focus most on the areas of highest risk.

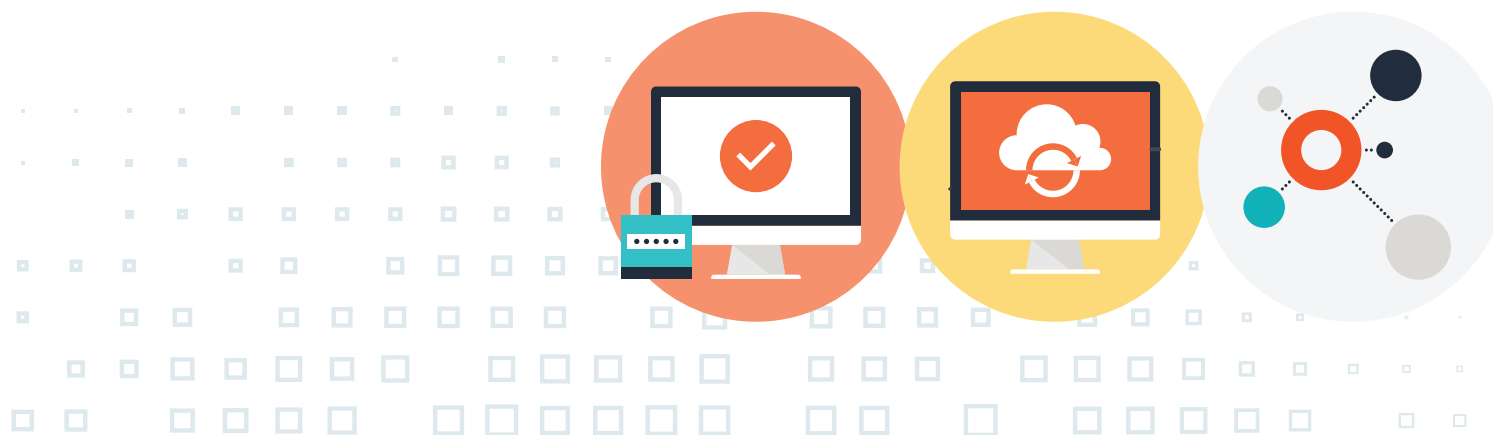
For this reason, it is unnecessary to test controls that, even if deficient, would not present a reasonable possibility of material misstatement to the financial statements. For example, suppose the inherent risk of fraud and error is less than reasonably possible, or the potential impact is not material. In that case, you don’t need a “key control” to reduce the likelihood of that risk.

To help you identify key controls, answer the following questions:

- Does the control mitigate the risk of a material misstatement originating from this business process?
- What if this control fails?

The first question seeks to clarify if you have identified a key risk by focusing on financials and materiality. If the control mitigates the identified risk of misstatement, it is a key control.

The second question addresses the possibility of another control overarching the failed control because only those controls at the top of the hierarchy are key controls.



What are SOX IT systems, and how to identify them?

To determine which systems are SOX IT systems, you need to distinguish whether they impact your financial reporting. For example, your CRM holds data critical to the operation of your business, but it does not capture data that feeds into or is used in financial reporting. Therefore, your CRM is not a SOX application. Internal controls should still govern your CRM, but your SOX auditors will not test these controls.

Examples of typical SOX IT systems:

- ERP
- Financial Consolidation and Disclosure systems
- Procurement Systems
- Human Resources Information Systems
- Accounting systems
- Revenue Recognition Systems



Limiting SOX controls

It can be tempting to apply a control to every identified risk. However, this leads to unnecessary and burdensome numbers of controls, which can be challenging to enforce and may needlessly impact operations.

Identifying your key controls helps you limit the number of controls to those necessary to address increased risk. A simple way to differentiate key controls vs. non-key controls is to evaluate the level of risk. If the risk is low, a control may not be needed.

Determining Materiality in SOX

Determining materiality is critical in understanding the level of controls required for a financial statement to comply with SOX. Because it is not practical for auditors to examine all transactions and balances, they focus on the areas that can significantly impact financial statements.

Materiality is the measure of importance that auditors use to determine a control's effect on a company's financials. Materiality is considered significant if it can influence the decision-making of those using the financial statements. There is no specific direction on determining materiality, and the process may differ depending on your accounting firm and your auditor's professional judgment.

However, auditors use estimates to help them identify potential material transactions and events. According to The Journal of Accountancy, "these estimates of materiality are typically based on the 5% rule, which maintains that reasonable investors would not be influenced in their investment decisions by a fluctuation in net income of 5% or less. Nor would the investor be swayed by a fluctuation or series of fluctuations of less than 5% in income statement line items as long as the net change was less than 5%."

The generally accepted levels that auditors utilize to benchmark materiality are:

- 5%-1% of total revenues or expenses
- 1%-2% of total assets
- 5%-10% of net profit before tax

SOX compliance requirements

SOX is long and complex piece of legislation, but there are four essential requirements:

- **Section 302** mandates that corporate officers, typically the CFO or CEO, certify that the company's financial statements comply with SEC requirements. Officers who sign off on financial statements they know to be false are subject to criminal penalties and prison.
- **Section 401** states that financial statements are accurate and prepared following GAAP accounting standards. Additionally, financial reports will include any off-balance-sheet transactions to ensure they meet the same standards.
- **Section 404** requires that management and auditors set internal controls and reporting procedures to ensure the adequacy of the controls.
- **Section 802** includes three rules that impact recordkeeping:
 1. Deals with the destruction and falsification of records.
 2. Strictly defines the retention period for keeping records.
 3. Outlines the records companies need to store, including electronic communications.



SOX IT compliance requirements

SOX compliance requirements also impact the company's IT department because they store the business's electronic records.

Section 404 focuses on auditing the company's internal controls, including the controls that govern its IT assets with access to financial data. SOX ITGC audits focus on four critical areas:

- **Access controls** like Segregation of Duties (SoD) prevent users without the proper authorization and credentials from gaining access to sensitive data, systems, and transactions. Identity governance (IGA) solutions and physical measures like restricted areas typically execute this function.
- **IT Security controls** ensure that computers, networks, and other devices where financial data flows are safeguarded to prevent breaches. These include password policies, security password policies across the enterprise, timely review and remediation of identities based on business justification for security, and device protection policies including encryption.
- **Change management controls** establish guidelines for updating systems and records with an audit trail of changes made. These include maintaining a log of changes to system configurations, patches, reports, workflows, interfaces and other programs that support your financial reporting.
- **Backup controls** ensure that financial systems have backups or can restore sensitive data. Both primary and backup systems must be SOX compliant.

Automated SOX controls

Your ERP is the most critical system under scrutiny during your SOX audit because it contains the most key controls. And of your key controls, SOX ITGCs make up a majority.

Manual testing of ITGCs in your ERP is a very tedious task. Reducing manual processes can significantly impact your SOX compliance costs. Manual processes require the involvement of employees or auditors and are not sustainable. In the long run, automated controls are more stable because they enable a repeatable, reliable, and predictable framework while lowering the cost of compliance.

Among the other benefits of automating your SOX and SOX IT controls are:

Continuous Controls Monitoring

Automated controls allow for Continuous Controls Monitoring (CCM). It is essential to ensure that the data entered in your ERP when onboarding a supplier for example, remains correct when it is time to pay invoices. Because the time between onboarding and payment can be lengthy, there is ample opportunity for internal and external bad actors to manipulate your data. CCM ensures that your data stays correct and up to date.

Increased efficiency

When a finance team is responsible for processing thousands of invoices, it can be a significant challenge to ensure that all the data in the invoices are correct. This process can consume many resources, including time and staff hours. Automated controls can shave hundreds of hours of manual checks, freeing your team to focus on other priorities.

Reduced fraud risk

Increasingly, organizations are concerned about insider threats. One malicious employee with elevated privileges can manipulate data in your ERP and perpetrate fraud against your organization. Identifying an employee engaged in fraud can take years to detect because they are adept at covering their tracks, know what manual controls are in place, and understand how to circumvent them. Automated controls can reduce this risk by limiting the access of staff members to data and systems that can be manipulated.

Improved security posture

Automated controls improve an organization's overall security posture. For instance, you can automate reminders to managers to test or execute a specific control and alert compliance officers when that work hasn't been completed. Reports from tests can be used in standard reports or risk dashboards to let you see and report security compliance quickly.

Increased cost-efficiency

The upfront costs of implementing automated controls may be higher than manual controls. However, over time automated controls are more cost-effective. Once an organization embraces automated controls, it can meet CCM and compliance obligations more efficiently. Automated controls also require fewer staff hours, saving you money.

Regulatory compliance

Reducing manual controls significantly impacts the SOX compliance costs of an organization. Manual processes requiring the involvement of employees or auditors are not sustainable. In the long run, automated controls are more stable because they enable a repeatable, reliable, and predictable framework while lowering the cost of compliance.

Automating SOX Controls with SafePaaS

SOX audit reporting is a stressful and arduous process. SafePaaS delivers continuous compliance by monitoring your SOX and SOX IT controls in real time with on-demand compliance reporting.

With SafePaaS, you'll pass your audit without surprises, with all potential risks secured before they materialize. And SafePaaS has integrations to all your critical financial applications that affect your SOX IT controls audit – Oracle, SAP, JD Edwards, PeopleSoft, NetSuite, Workday, and more.

With SafePaaS' seamless API integrations to your ERP application, you can choose from our comprehensive repository of predefined, industry-best-practice rules. SafePaaS locks down all your SOX and SOX IT controls so you can concentrate on your business, not your audit.

Continuous Controls Monitoring

SafePaaS monitors and identifies risks in financial transactions from applications like Oracle ERP Cloud and E-Business Suite and remediates them with built-in remediation capabilities.

Risk-impact on finances

With the use of automation, you can prioritize your most important policy violations by measuring access risk-to-cost.

Best-practice industry-focused rule catalog

SafePaaS has thousands of rules that provide immediate coverage of your compliance requirements, including SOX, GDPR, and HIPAA.

Real-time access risk mitigation

SafePaaS enables quick analysis and response to potential risk by reviewing identity access in real time with fine-grained capabilities.

Out-of-the-Box Integrations

SafePaaS API integrations enable provisioning workflows with ServiceNow, Okta, Azure AD, or any other IDM and ITSM.

Cross-application SOD analysis

All entitlements and roles are analyzed across all applications in one single platform.

To learn more about how SafePaaS can help you automate SOX controls, please, [contact us](#).

3300, Dallas Parkway, Suite 200, Plano, Texas, 75093 USA