ConductorOne

SOX Audit: Who Needs It, When, and How to Prepare

*The **Sarbanes-Oxley (SOX) Act**, signed into law in 2002, is a comprehensive piece of legislation created to protect investors by improving the accuracy and reliability of corporate disclosures in financial statements and other significant reporting.*

What is a SOX audit?

A SOX **audit**, also known as a Sarbanes-Oxley audit, is an essential compliance process that all publicly traded companies in the United States must undergo to adhere to the regulations established by the Sarbanes-Oxley Act of 2002.

The goal of a SOX audit is simple: **verify the accuracy of a company's financial statements and make sure the company has strong internal controls in place to prevent errors or corporate fraud.**

Objectives of a SOX audit

→ **Assessing internal controls**. A significant part of a SOX audit involves evaluating the effectiveness of a company's internal controls over financial reporting. Independent external auditors check if controls are properly designed, implemented, and maintained to prevent and detect errors or fraud in financial reporting.

→ **Verifying financial statements**. Auditors also review a company's financial statements to ensure they are free of material misstatement and that they accurately reflect the company's financial condition in accordance with generally accepted accounting principles (GAAP).

→ **Testing compliance**. The audit tests compliance with SOX's various requirements, including those related to financial disclosures, internal control procedures, and corporate governance.

What does a SOX audit involve?

1. Defining the audit scope

The audit begins with the auditors gaining a thorough understanding of the company's operations. This involves identifying the key financial processes, systems, and controls.

The auditors conduct a risk assessment to pinpoint areas within the financial reporting that are most vulnerable to errors or fraudulent activities. This risk-based approach helps in determining the scope of the audit and focusing on high-risk areas.

2. Materiality and risk assessment

In this step, auditors evaluate the materiality of various financial accounts, statements, and business processes. They also identify high-risk areas where internal controls are critical. This includes factors such as the size and complexity of transactions and the susceptibility to manipulation.

> 💡 **Materiality** refers to the significance of an item or error that could influence the economic decisions of users of the financial statements.

3. Identifying SOX controls

Auditors identify and review different types of internal controls to ensure their effectiveness. These include:

→ **IT general controls (ITGCs)**. These controls ensure the overall security, integrity, and reliability of the IT infrastructure used in financial reporting. They include access controls, change management, and data backup procedures.

→ **Application controls**. These are specific controls within financial reporting software that ensure the accuracy and completeness of transaction processing and data integrity.

→ **Entity level controls**. These broad organizational controls cover aspects like segregation of duties (SoD), governance, and oversight mechanisms. They ensure that no single individual has control over all aspects of any critical financial process — this way, reducing the risk of fraud.

4. Fraud risk assessment

The auditors assess the company's exposure to fraud risks. They evaluate the effectiveness of controls designed to prevent and detect fraudulent activities.

This includes reviewing anti-fraud programs, conducting interviews with management and staff, and examining the company's culture and ethical practices.

5. Process and control documentation review

Auditors review the documentation that describes the company's internal controls and their implementation.

This documentation includes policies, procedures, flowcharts, and control matrices. The aim is to ensure that controls are well documented, consistently applied, and effectively communicated throughout the organization.

6. Testing key controls

Auditors employ various techniques to test the effectiveness of key controls. This involves selecting a sample of transactions and verifying that controls are applied consistently and operate as intended.

Testing can include reviewing financial transactions, inspecting documentation, observing processes, and interviewing personnel involved in the financial reporting process.

7. Assessing deficiencies

Based on the results of control testing, auditors identify any deficiencies or gaps in the internal control framework.

These deficiencies are categorized as either control deficiencies, significant deficiencies, or material weaknesses, depending on their severity and potential impact on the financial statements.

8. Delivering reports

The final phase of a SOX audit is reporting. Auditors prepare a detailed report outlining their findings, including any identified deficiencies and the effectiveness of the company's internal controls over financial reporting.

The audited company gets two key reports:

→ **Management's report on internal controls**. Prepared by the company's management, this report acknowledges their responsibility for establishing and maintaining effective internal controls. It includes an assessment of the effectiveness of the internal control framework and discloses any identified weaknesses along with planned remediation efforts.

→ **Auditor's report on internal control over financial reporting**. This independent report provides the auditor's opinion on the effectiveness of the company's internal controls over financial reporting. It highlights any material weaknesses or significant deficiencies identified during the audit.

The company then shares this report with its management, audit committee, and external stakeholders.

> 💡 **Note →** Public companies must include a section on internal control over financial reporting in their annual reports, and the external auditor's attestation on management's assessment.

What types of organizations need SOX auditing?

The Sarbanes-Oxley Act (SOX) primarily targets publicly traded companies, but its impact and relevance extend beyond this scope to other types of organizations.

Here's a detailed look at the various types of organizations that require SOX auditing:

→ **Publicly traded companies**. This applies to all companies listed on major US stock exchanges, including their wholly owned subsidiaries. This requirement ensures transparency, reliability, and accuracy in their financial statements, which is crucial for maintaining investor confidence and protecting shareholders.

Key requirements for publicly traded companies include:

- **Section 302**. Senior executives must certify the accuracy of financial statements and the effectiveness of internal controls.

- **Section 404**. Management and external auditors must report on the adequacy of the company's internal control over financial reporting (ICFR).

→ **Publicly traded non-US companies**. Foreign companies that have securities listed on US stock exchanges are also subject to SOX requirements. These companies must adhere to the same internal control and financial reporting standards as their US counterparts.

→ **Private companies planning to go public/IPO**. Private companies that are preparing for an initial public offering (IPO) must comply with SOX regulations. This preparation often includes implementing robust internal controls and undergoing SOX audits to ensure that their financial reporting meets the stringent requirements of public markets.

→ **Accounting firms and third-party service providers**.

- **Accounting Firms**. Public accounting firms that audit the financial statements of publicly traded companies must comply with SOX standards to ensure the accuracy and integrity of their audits. The Public Company Accounting Oversight Board (PCAOB) oversees these firms, setting auditing standards and inspecting audits to ensure compliance.

- **Third-party service providers**. Companies often rely on third-party service providers for various functions, such as IT services, payroll processing, and financial data management. These service providers must maintain robust internal controls and undergo independent audits to ensure they meet the necessary standards for their clients' SOX compliance. Failure to do so can lead to significant risks for their clients and impact the overall integrity of the financial reporting process.

→ **Large nonprofits with complex finances**. Large nonprofit organizations with complex financial structures may also adopt SOX-like internal control frameworks. These nonprofits, often handling substantial amounts of funding from various sources such as government grants, private donations, and endowments, face significant pressure to ensure transparency and accountability in their financial reporting.

💡 **Pro Tip →** ConductorOne lets you track population reports, access certification results, and remediation activity and produce accurate, auditor-loved reports in a click.

When should a private company perform a SOX audit?

While private companies are not legally required to comply with the Sarbanes-Oxley Act (SOX), there are several situations where performing a SOX audit can be beneficial and strategically important.

→ **Third-party insistence**. In some cases, third-party entities such as major customers, suppliers, or business partners may insist on SOX compliance as a condition of doing business. These third parties may require assurance that the company’s financial reporting and internal controls meet high standards of transparency and reliability. Performing a SOX audit in such cases can help secure and maintain important business relationships, demonstrating the company’s commitment to robust financial governance.

→ **Due diligence for investment or acquisition**. Private companies looking to attract investment from venture capitalists or private equity firms, or considering a potential acquisition, can benefit from SOX compliance. Demonstrating strong internal controls and transparent financial reporting can enhance the company’s attractiveness to investors and acquirers. It provides assurance that the company’s financial statements are accurate and reliable, reducing perceived risks and increasing investor confidence.

→ **Loan applications**. When applying for substantial loans or lines of credit, private companies may find that lenders require proof of strong internal controls and reliable financial reporting. Compliance with SOX can provide lenders with the assurance that the company has effective mechanisms in place to manage financial risks and ensure the accuracy of financial information. This can enhance the company’s creditworthiness and increase the likelihood of securing favorable loan terms.

→ **Building trust and credibility.** Even without a legal requirement, private companies may choose to perform a SOX audit to strengthen their internal controls and risk management practices. This approach helps identify and address weaknesses in financial reporting processes, reduces the risk of fraud and errors, and improves overall operational efficiency.

→ **Preparing for an initial public offering (IPO)**. Private companies planning to go public through an IPO must comply with SOX regulations once they become publicly traded. Starting SOX compliance efforts early ensures a smoother transition to public company status. Implementing robust internal controls and undergoing SOX audits can help the company meet the stringent financial reporting standards required for an IPO, build credibility with potential investors, and avoid delays in the IPO process.

How to prepare for a SOX compliance audit [a complete checklist]

Step 1 → Understand the requirements

Step 2 → Establish a compliance team

Step 3 → Document processes and controls

Step 4 → Test controls

Step 5 → Review IT systems

Step 6 → Perform a pre-audit review

Step 7 → Coordinate with external auditors

Step 1 Understand the requirements

→ Understand the key provisions of the Sarbanes-Oxley Act, particularly Sections 302 and 404 (*more on this below*), which deal with internal control requirements and the responsibilities of senior management.

→ Then, determine which controls are applicable to your organization's financial reporting processes.

Step 2 Establish a compliance team

→ Form a compliance team that includes members from finance, IT, HR, and any other departments involved in financial reporting.

→ If not already done, hire an external auditing firm that specializes in SOX compliance.

→ Ensure clear communication channels exist between various departments involved in financial reporting. This makes it easy to identify potential issues before they become major.

Step 3 Document processes and controls

→ Document all processes related to financial reporting, including data collection, data processing, and data reporting.

→ Develop detailed narratives that explain how your internal controls work and their role in safeguarding financial data.

→ Create visual aids like flowcharts or process maps to illustrate the flow of financial records and how controls are applied at each stage.

Step 4 Test controls

→ Have the internal audit team or an external consultant test the effectiveness of the controls. This should be done well before the external auditors conduct their tests.

Step 5 Review IT systems

→ Given that financial data is often processed and stored electronically, evaluate the controls over IT systems and data security.

- If needed, enhance IT security measures and system controls to comply with SOX requirements.

Step 6 Perform a pre-audit review

→ Simulate an external audit with your internal audit team to identify any potential issues.

→ Make any necessary adjustments to processes and controls based on the findings of the pre-audit.

Step 7 Coordinate with external auditors

→ Schedule introductory meetings with the external auditors to understand their expectations and timeline for the audit.

→ Designate a knowledgeable point of contact within your company to facilitate communication and address any questions from the auditors.

- If necessary, consider seeking professional guidance from SOX compliance consultants to ensure a smooth audit process.

SOX compliance requirements

SOX is comprehensive, consisting of 11 titles, each addressing different facets of corporate governance, financial reporting, and audit procedures.

However, there are two key provisions in terms of compliance requirements:

Corporate responsibility for financial reports (Section 302)

- → **CEO and CFO certifications**. The chief executive officer (CEO) and chief financial officer (CFO) must certify the accuracy of financial reports. This includes affirming that they have reviewed the report, it does not contain any false information or omit significant facts, and it fairly presents the financial condition of the company.
- → **Internal controls**. They must also certify the effectiveness of internal controls over financial reporting and disclose any recent material changes in these controls.

Read SOX Section 302 in detail.

Management assessment of internal controls (Section 404)

- → **Internal control report**. Companies must include an internal control report with their annual financial report. This report must affirm the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.
- → **Auditor evaluation**. The company's external auditor must attest to and report on the assessment made by the management. This includes an evaluation of the effectiveness of the internal control structure and procedures for financial reporting.

Read SOX Section 404 in detail.

Importance of SOX sections 302 and 404 in ensuring accurate financial reporting

Together, Sections 302 and 404 of the SOX Act ensure the accuracy and reliability of financial reporting through stringent internal controls.

This is particularly important in ensuring the integrity of financial data (like balance sheets) and the systems in which it resides — in this case, IT controls.

Here's how it works:

- → **Focus on monitoring and logging**.
  - User login attempts (successes and failures)
  - Network activity (data transfers, access attempts)
  - Database activity (data modifications, access logs)
  - Account activity within financial systems
  - Information access attempts (who is trying to access what data)

→ **Log collection and monitoring systems**. IT departments must have systems in place to collect and monitor these logs. These systems should provide a comprehensive audit trail of all activity related to financial data. This allows auditors to reconstruct events and verify the effectiveness of IT controls.

→ **Adopt a control framework**. A documented framework like COBIT to help organize and assess the effectiveness of IT controls related to SOX compliance.

💡 **COBIT** (Control Objectives for Information and Related Technology) is a framework designed to help businesses develop, implement, monitor, and improve IT governance and management practices

→ **Security**. To safeguard financial data, companies implement robust security measures including:

- **Data security**. Uses advanced data security measures like encryption to prevent unauthorized access, data breaches, and cyberattacks.
- **Access controls**. Enforces strict controls over who can view or modify financial data, minimizing risks of insider threats.
- **Data backups**. Ensures regular backups of financial data to secure locations for recovery after incidents.
- **Change management**. Manages changes to IT infrastructure in a controlled manner, ensuring all modifications are justified, documented, and traceable.

SOX Compliance Checklist

Prevent Data Tampering (302.2)

Establish Timelines (302.3)

Track Data Access (302.4.B)

Ensure Safeguard Operation (302.4.C)

Report Safeguard Effectiveness (302.4.D)

Detect Security Breaches (302.5.A/B)

Disclose Safeguards to Auditors (404.A.1.1)

Disclose Security Breaches (404.A.2)

Disclose Safeguard Failures (404.B)

Prevent data tampering (302.2)

→ Implement comprehensive logging mechanisms to monitor user activity, such as logins and access attempts across all devices containing sensitive data.

→ Set up alerts for suspicious activities such as multiple failed login attempts, unusual access patterns, or unauthorized data modifications.

💡 **Tip →** Use advanced logging tools to capture detailed information about each login attempt, including timestamps, user IDs, device identifiers, and IP addresses.

Establish timelines (302.3)

→ Ensure that all incoming data is automatically timestamped to maintain a chronological record.

→ Implement processes to securely transfer and store data at a remote location as soon as it is received.

→ Use cryptographic techniques to protect log data and ensure its integrity.

- Implement encrypted checksums or hash values for log entries to detect any tampering.

💡 **Tip →** You can synchronize system clocks across all servers and devices using Network Time Protocol (NTP) to ensure accurate timestamps.

Track data access (302.4.B)

→ Set up a system capable of aggregating data from different sources such as file queues, FTP, and databases.

→ Ensure your data collection system is independent and not tied to specific frameworks like COSO, COBIT, or ITGI.

- COSO (Committee of Sponsoring Organizations of the Treadway Commission) is an organization that provides guidance on organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting.
- ITGI (IT Governance Institute) helps organizations understand and manage the risks and benefits associated with information technology.

💡 **Tip →** Ensure the system is scalable and can handle data from multiple sources simultaneously without performance degradation.

Ensure safeguard operation (302.4.C)

Set up automated systems to distribute security and operational reports through RSS feeds and daily email alerts.

💡 **Tip →** Regularly verify the functionality of these systems to ensure they generate and distribute reports as expected.

Report safeguard effectiveness (302.4.D)

→ Develop a reporting system that provides detailed insights into messages, critical messages, alerts, and overall security activities.

→ Implement a ticketing system to document and track security issues, including actions taken to resolve them.

💡 **Tip →** Maintain a comprehensive archive for audit purposes and future reference.

Detect security breaches (302.5.A/B)

→ Use real-time semantic analysis to examine messages for signs of security breaches.

→ Utilize correlation, counters, and alerts to filter and refine cybersecurity incidents into actionable alerts.

→ Automatically generate tickets for detected security breaches to notify personnel and update incident management systems.

💡 **Tip →** Regularly review and update alerting rules to minimize false positives and negatives.

Disclose safeguards to auditors (404.A.1.1)

Implement role-based access controls (RBAC) to provide auditors with specific, read-only access to reports and facilities.

💡 **Tip →** Regularly review and update access permissions to ensure compliance and security.

Disclose security breaches (404.A.2)

→ Set up systems to detect, log, and promptly notify security personnel of any security breaches.

→ Implement a system to record and store resolutions to security incidents for future analysis.

💡 **Tip →** Ensure notifications include detailed information to facilitate a quick and effective response.

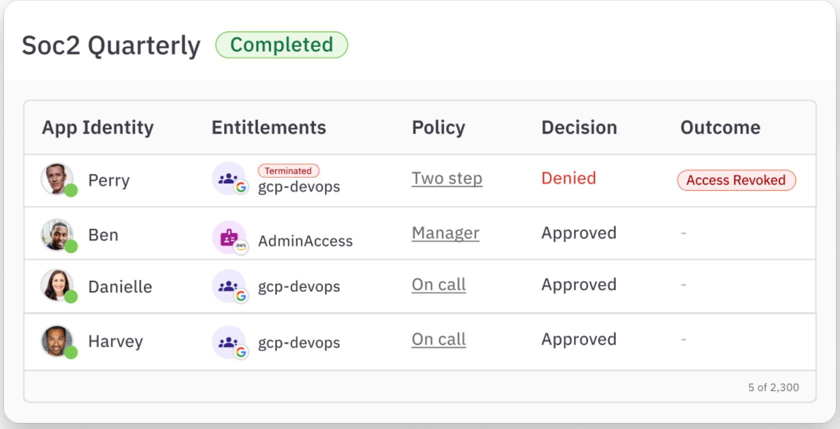
Disclose safeguard failures (404.B)

→ Set up a system to conduct regular tests of network and file integrity, ensuring message logging accuracy.

→ Use security testing software and port scanners to continuously monitor IT security and identify potential threats.

💡 **Tip →** Automate scans and integrate findings into your overall security management strategy.

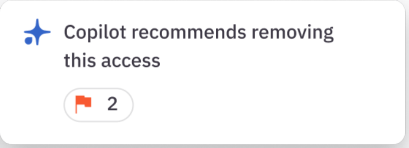
Streamline SOX control auditing with ConductorOne



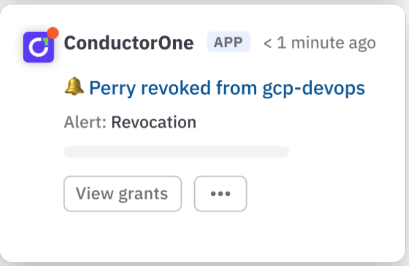
Soc2 Quarterly Completed

App Identity	Entitlements	Policy	Decision	Outcome
Perry	Terminated gcp-devops	Two step	Denied	Access Revoked
Ben	AdminAccess	Manager	Approved	-
Danielle	gcp-devops	On call	Approved	-
Harvey	gcp-devops	On call	Approved	-

5 of 2,300



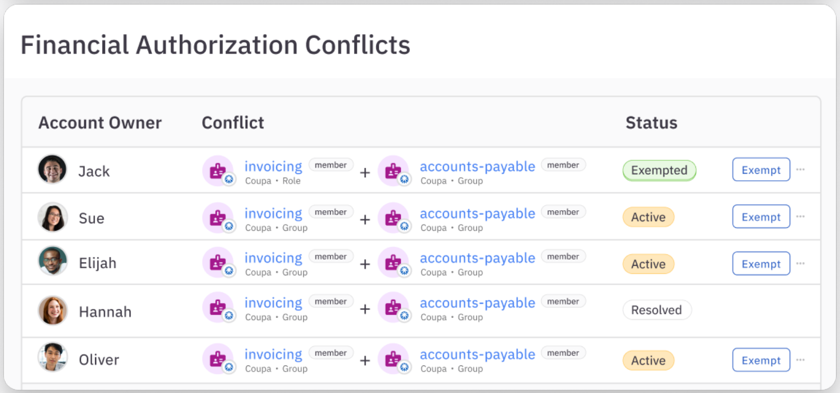
Copilot recommends removing this access



ConductorOne APP < 1 minute ago

🔔 Perry revoked from gcp-devops

Alert: Revocation



Financial Authorization Conflicts

Account Owner	Conflict	Status	
Jack	invoicing member Coupa • Role + accounts-payable member Coupa • Group	Exempted	Exempt ···
Sue	invoicing member Coupa • Group + accounts-payable member Coupa • Group	Active	Exempt ···
Elijah	invoicing member Coupa • Group + accounts-payable member Coupa • Group	Active	Exempt ···
Hannah	invoicing member Coupa • Group + accounts-payable member Coupa • Group	Resolved	
Oliver	invoicing member Coupa • Group + accounts-payable member Coupa • Group	Active	Exempt ···

Manual processes and scattered data can make SOX compliance a headache. ConductorOne simplifies SOX preparation by automating key tasks, giving you real-time visibility, and making team collaboration a breeze.

Case Study → How System1 manages disparate systems after M&A activity and streamlined SOX audits.

SOX audit — the way auditors love it

→ **Automated evidence collection**. Forget manual data collection. ConductorOne gathers all the evidence you need automatically, saving time and reducing errors.

→ **Real-time monitoring**. Stay on top of control effectiveness with real-time dashboards. Instantly see what's working and what needs attention.

→ **Simplified collaboration**. Keep everyone in the loop with streamlined communication tools. ConductorOne makes it easy for teams to work together on compliance tasks.

→ **Continuous monitoring**. Spot and fix control issues year-round with continuous monitoring. Stay compliant without the last-minute scramble.

→ **Audit trail management**. Maintain a secure, tamper-proof audit trail with automated evidence collection. Every action is logged and easy to review.

Take the stress out of SOX compliance with ConductorOne. Automate tasks, enhance team collaboration, and ensure continuous compliance effortlessly.

> "Being able to show ConductorOne to internal auditors, where they can generate time-stamped, immutable reports, and see logs in one console, was impressive."
>
> **Jack Chen**
> Director of Information Technology, SYSTEM

Ready to simplify SOX compliance?

Schedule a demo with ConductorOne today!

Get a demo