

Sarbanes-Oxley Act (SOX) - Pub. L. No. 107-204 (2002)

The Sarbanes-Oxley Act requires public companies to maintain reliable financial reporting and robust internal controls to prevent fraud.



What it is

The Sarbanes-Oxley Act (SOX) is a U.S. federal regulation that establishes rigorous requirements for financial reporting, internal controls, and compliance oversight to enhance corporate accountability and prevent financial fraud. Originally enacted in 2002 in response to major corporate scandals, SOX aims to strengthen transparency and reliability in financial disclosures for public companies.

Published and enforced by U.S. Congress and federal regulatory agencies such as the Securities and Exchange Commission (SEC), SOX applies primarily to publicly traded companies, their auditors, and certain subsidiaries. The Act addresses areas such as internal control over financial reporting, cybersecurity risk management, audit trails, and executive accountability for financial statements.

At a glance

PUBLISHER U.S. Securities and Exchange Commission (SEC)	TYPE Regulation	VERSION Sarbanes-Oxley Act of 2002
EFFECTIVE July 30, 2002	DOMAIN Financial Services Regulation	FAMILY COSO
REGION United States	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <http://www.sec.gov/about/laws/soa2002.pdf>

Why it matters

- Enhance financial reporting integrity** Strengthen the accuracy and reliability of financial disclosures to improve shareholder and stakeholder trust.
- Increase audit readiness** Enable comprehensive internal controls and documentation that streamline audit processes and support independent verification.
- Strengthen executive accountability** Hold company leadership directly responsible for financial statements, fostering a culture of ethical governance and compliance.
- Protect sensitive financial data** Increase safeguards around financial information, reducing the risk of cyber threats, data breaches, and internal misuse.

How SmartSuite supports SOX

ICFR Control Library and RCMs

Manage SOX controls, process narratives, and RCMs with clear ownership.

ITGC Tracking and Evidence

Run access, change management, and operations control evidence collection at scale.

Testing Cycles and Operating Effectiveness

Plan testing, document results, and track exceptions through remediation.

Deficiency and Remediation Workflow

Manage deficiencies, action plans, retesting, and closure verification.

Cross-Team Evidence Coordination

Centralize evidence sources and approvals across Finance, IT, and Security teams.

Auditor and Leadership Reporting

Provide audit-ready dashboards across controls, testing status, and open issues.

Common framework mappings

- Basel III
- COBIT 2019
- ISO 27001:2022
- NIST CSF 2.0
- SOC 1

Official resources

Sarbanes-Oxley Act of 2002

Official publication of the Sarbanes-Oxley Act outlining corporate financial accountability and transparency requirements.
sec.gov/about/laws/soa2002.pdf

SEC SOX Section 404 Guidance

Provides guidelines for management's assessment of internal control over financial reporting.
sec.gov/info/accountants/controlfaq.htm

Public Company Accounting Oversight Board (PCAOB) Standards

Defines auditing standards for improving the accuracy and reliability of company disclosures.
pcaobus.org/Standards

SEC Financial Reporting Manual

Outlines financial reporting requirements for public companies under SOX.
sec.gov/corpfin/cf-manual

Frequently asked questions

What is the Sarbanes-Oxley Act (SOX) used for?

SOX is designed to enhance the accuracy and reliability of financial reporting by requiring public companies to implement and maintain robust internal controls. The Act aims to prevent financial fraud, promote transparency, and ensure executive accountability in financial disclosures.

Is SOX compliance mandatory?

Yes, SOX compliance is mandatory for all publicly traded companies in the United States, including their subsidiaries and external auditors. Privately held companies are not generally required to comply but may adopt SOX controls voluntarily for best practices.

Who does SOX apply to?

SOX primarily applies to companies listed on U.S. stock exchanges, their executives, board members, auditors, and certain subsidiaries. Foreign companies with securities listed in the U.S. are also subject to SOX requirements.

What key controls and documentation does SOX require?

SOX requires organizations to establish and document internal controls over financial reporting (ICFR), including processes for recording transactions and safeguarding financial data. Required artifacts include control matrices, process documentation, risk assessments, audit trails, and testing evidence.

How do organizations implement SOX compliance in practice?

Organizations implement SOX by designing internal control frameworks, regularly testing and reviewing control effectiveness, and documenting results. Ongoing executive certifications and independent external audits are essential components of SOX compliance programs.

How does SOX relate to IT security and other compliance frameworks?

SOX compliance increasingly intersects with IT security due to the reliance on information systems for financial reporting. While SOX focuses on financial controls, its principles are often integrated with broader governance, risk management, and security standards such as COSO and COBIT.

What are the ongoing requirements to remain SOX compliant?

To maintain SOX compliance, organizations must continuously monitor and test internal controls, promptly remediate control deficiencies, retain supporting documentation, and ensure executives certify the effectiveness of controls at year-end. Annual external audits provide independent verification of compliance.

How would SmartSuite support SOX (Sarbanes-Oxley Act)?

SmartSuite enables organizations to manage SOX compliance by centralizing control documentation, tracking control testing activities, and facilitating continuous risk assessments. It also supports the collection and retention of audit evidence, enhances audit readiness, and provides reporting tools to monitor compliance status and remediation efforts.

License included / downloadable: Yes The Sarbanes-Oxley Act is U.S. federal legislation and is publicly available through official government publications.

Full framework page and mappings: smartsuite.com/frameworks/sox-sarbanes-oxley-act