SmartSuite

Framework / Other / Other

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

The Sarbanes-Oxley Act of 2002 (Public Law 107-204) requires SEC-reporting companies to certify reports, assess internal control over financial reporting and use PCAOB-registered auditors.



What it is

The Sarbanes-Oxley Act of 2002 (SOX, Public Law 107-204, 116 Stat. 745) is the United States federal law that makes the chief executive and chief financial officers of every SEC-reporting company personally certify their periodic reports (section 302), requires management's annual assessment of internal control over financial reporting with an auditor's attestation for larger filers (section 404), and polices the auditors through the Public Company Accounting Oversight Board (Title I). Congress enacted it on July 30, 2002, and it binds every issuer that files reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934.

At a glance

PUBLISHER
United States Congress (Public Law 107-204); administered by the Securities and Exchange Commission and the Public Company Accounting Oversight Board

TYPE
Regulation

VERSION
Public Law 107-204, 116 Stat. 745 (2002), as amended by the Dodd-Frank Act section 989G (2010) and the JOBS Act section 103 (2012)

EFFECTIVE
July 30, 2002 (enactment; SEC implementing rules phased in afterward)

DOMAIN
Other

FAMILY
Other

REGION
United States

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: govinfo.gov/app/details/PLAW-107publ204

Why it matters

- **Personal certification** Section 302 requires the principal executive and financial officers to certify each annual and quarterly report, including that they evaluated the effectiveness of internal controls within 90 days of the report.
- **A documented control assessment** Section 404(a) requires management's annual report on the adequacy of the internal control structure and an assessment of its effectiveness as of fiscal year-end.
- **Independent attestation** Section 404(b) requires the registered public accounting firm to attest to and report on management's assessment, under PCAOB standards, unless section 404(c) or the emerging growth company exclusion applies.
- **Auditor independence** Section 201 bans nine non-audit services for audit clients, section 202 requires audit committee preapproval of the rest, and section 203 rotates the lead and reviewing partners after five years.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports SOX

ICFR Control Library and RCMs

Hold key controls, process narratives and risk and control matrices by financial statement assertion, with the control framework named in the Item 308 report and clear ownership.

ITGC Scoping and Evidence

Track access, change management and operations controls for the in-scope financial applications and the service organizations whose SOC 1 reports the auditors rely on, with complementary user entity controls assigned.

Testing Cycles and Operating Effectiveness

Plan design and operating effectiveness testing to the fiscal year-end assessment date, record samples and results, and track exceptions through retesting.

Deficiency Evaluation and Remediation

Classify deficiencies, significant deficiencies and material weaknesses, link remediation plans and closure evidence, and carry open items into the section 302 disclosure to the audit committee.

Section 302 and 906 Certification Workflow

Run quarterly sub-certifications from process owners up to the principal executive and financial officers, with the 90-day evaluation conclusions and changes in internal control recorded.

Audit Committee and Auditor Reporting

Report control status, testing progress, open deficiencies and remediation to the audit committee under section 301 and give the external auditor one evidence source for the AS 2201 integrated audit.

Common framework mappings

Basel III | COBIT 2019 | COSO IC 2013 | ISO 27001:2022 | NIST CSF 2.0 | PCAOB AS 2201 | SOC 1

Official resources

Public Law 107-204, Sarbanes-Oxley Act of 2002 (govinfo)

The enacted text of the Act, 116 Stat. 745, from the U.S. Government Publishing Office.

govinfo.gov/app/details/PLAW-107publ204

SEC SOX Section 404 Guidance

Provides guidelines for management's assessment of internal control over financial reporting.

sec.gov/info/accountants/controlfaq.htm

PCAOB AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements

The PCAOB standard for the section 404(b) auditor attestation.

pcaobus.org/oversight/standards/auditing-standards/details/AS2201

SEC Financial Reporting Manual

Outlines financial reporting requirements for public companies under SOX.

sec.gov/corpfin/cf-manual

Frequently asked questions

Which companies does the Sarbanes-Oxley Act apply to?

Section 2 defines an issuer as a company whose securities are registered under section 12 of the Securities Exchange Act of 1934, that must file reports under section 15(d), or that has a registration statement pending, which covers domestic public companies and foreign private issuers listed in the United States. The Act also binds their officers, directors and audit committees and the registered public accounting firms that audit them. Section 405 exempts registered investment companies from sections 401, 402 and 404.

What do sections 302 and 906 require the CEO and CFO to certify?

Section 302 requires the principal executive and financial officers to certify in each annual and quarterly report that they reviewed it, that it contains no material misstatement or omission, that the financial statements fairly present the issuer's condition, that they are responsible for internal controls and evaluated their effectiveness within 90 days of the report, and that they disclosed significant deficiencies, material weaknesses and fraud to the auditors and audit committee. Section 906 adds the criminal certification of 18 U.S.C. 1350: a knowing false certification carries up to $1 million and ten years, a willful one up to $5 million and twenty years.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What is the difference between section 404(a) and section 404(b)?

Section 404(a) requires management's internal control report in every annual report: a statement of management's responsibility for adequate internal control over financial reporting and an assessment of its effectiveness as of fiscal year-end, made against a suitable framework named in the report under Regulation S-K Item 308. Section 404(b) requires the issuer's registered public accounting firm to attest to and report on that assessment under PCAOB standards; it applies only to accelerated and large accelerated filers that are not emerging growth companies.

Who is exempt from the section 404(b) auditor attestation?

Section 404(c), added by section 989G of the Dodd-Frank Act in 2010, exempts issuers that are neither accelerated nor large accelerated filers under Exchange Act Rule 12b-2, and section 103 of the JOBS Act of 2012 exempts emerging growth companies. The SEC's amendments of March 12, 2020 (Release 34-88365) removed from the accelerated filer definitions issuers eligible to be smaller reporting companies with annual revenues under $100 million, so they keep the management assessment but not the attestation.

How long must audit records be kept under SOX?

Section 802 added 18 U.S.C. 1520, which requires any accountant who audits an issuer to keep all audit or review workpapers for five years from the end of the fiscal period in which the audit was concluded, with up to ten years' imprisonment for a knowing and willful violation. The SEC's implementing Rule 2-06 of Regulation S-X extends the retention of workpapers and other records relevant to the audit to seven years after the audit or review is concluded.

License included / downloadable: Yes The Act is a United States public law published free on govinfo.gov and congress.gov; the platform links to the official text.

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

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.