COMPLIANCE CHECKLIST

SOX compliance checklist

Sarbanes-Oxley Act of 2002

Jurisdiction: US public companies (and their material subsidiaries)

Programme details

ORGANISATION NAME

[Organisation name]

ASSIGNED TO

[Assigned to]

TARGET COMPLETION DATE

[Target completion date]

REVIEWED BY

[Reviewed by]

REVIEW DATE

[Date]

Who SOX applies to

US public companies that file annual reports with the SEC (and their material subsidiaries). SOX Section 404(a) applies to all SEC filers; Section 404(b) external-auditor attestation applies to accelerated filers and large accelerated filers only. Three populations are exempt: non-accelerated filers have always been exempt; smaller reporting companies with annual revenues below $100M were carved out by the SEC's 2020 amendments to the accelerated-filer definitions; and emerging growth companies are exempt for up to five years post-IPO under the 2012 JOBS Act.

SOX checklist

STEP 1

- [ ] Identify significant accounts, processes, and locations in the SOX scope each year.

STEP 2

- [ ] Identify IT General Controls (ITGCs) for the systems supporting financial reporting.

STEP 3

- [ ] Document control design - risk-control matrix, control owners, frequency, evidence.

STEP 4

- [ ] Map controls to COSO 2013 internal-control framework components.

STEP 5

- [ ] Perform walkthroughs to confirm design as documented.

STEP 6

- [ ] Test operating effectiveness across the year - sample size driven by frequency.

STEP 7

- [ ] Evaluate findings; remediate and re-test before year-end.

STEP 8

- [ ] Issue management's Section 404(a) assertion on ICFR effectiveness.

STEP 9

- [ ] External auditor performs the Section 404(b) integrated audit (where applicable).

STEP 10

- [ ] File the 10-K with management assertion and auditor opinion.

FAQ

What is SOX Section 404?

Section 404 of the Sarbanes-Oxley Act requires US public companies to assess and report on the effectiveness of their internal controls over financial reporting. Section 404(a) is management's assessment and applies to all SEC filers. Section 404(b) is the integrated audit performed by the external auditor and applies only to accelerated and large accelerated filers. Non-accelerated filers have always been exempt; smaller reporting companies under $100M in revenue were carved out by the SEC's 2020 amendments; emerging growth companies have a separate 5-year post-IPO exemption under the JOBS Act.

How does SOX interact with COSO and PCAOB AS 2201?

COSO 2013 is the most widely used framework for the internal control structure. PCAOB Auditing Standard 2201 governs how the external auditor conducts the integrated audit. A SOX programme typically maps each significant control to a COSO component and follows AS 2201 logic for testing depth.

What are ITGCs?

IT General Controls - the controls over the IT environment that support reliable processing for the financial-reporting systems. The classic ITGC categories are access management, change management, IT operations, and program development.

How long does a SOX programme take to build from scratch?

A first-year SOX programme typically takes 9-12 months from scoping to auditor walkthrough. The cadence shortens after Year 1 because the scope, control documentation, and testing approach roll forward - but the testing window remains the binding constraint.

Source: https://ba-copilot.com/compliance/sox-compliance-checklist. Tick each item as it is completed and add the named owner.