SOX Compliance Checklist

Checklist · 95 items · 14 sections

A practical SOX compliance checklist for CFOs, controllers, and internal audit leaders at US public companies. Covers Section 302 and 404 certifications, the COSO 2013 internal control framework, ITGCs, key process controls, and PCAOB-aligned testing.

Open the editable, AI-powered version online:
https://genechecklist.com/checklist/sox-compliance-checklist

SOX FUNDAMENTALS

- [ ] Confirm SOX applicability: all US public companies registered with the SEC, plus their PCAOB-registered external auditors

  HIGH

- [ ] Identify filer status (large accelerated, accelerated, non-accelerated, EGC)

  HIGH

  404(b) auditor attestation is required only for accelerated and large accelerated filers.

- [ ] Confirm EGC (Emerging Growth Company) status under the JOBS Act if applicable

  HIGH

  EGCs are exempt from 404(b) for up to 5 years post-IPO.

- [ ] Designate SOX executive sponsor (typically CFO), with controller or VP Internal Audit as program owner

  HIGH

- [ ] Maintain a SOX charter approved by the audit committee defining scope, roles, and reporting cadence
- [ ] Brief the audit committee at least quarterly on SOX status, deficiencies, and remediation

SECTION 302 CERTIFICATIONS

- [ ] Have CEO and CFO personally sign Section 302 certifications with every 10-Q and 10-K

  HIGH

- [ ] Certify that the report does not contain any untrue statement of material fact or omit a material fact

  HIGH

- [ ] Certify that financial statements fairly present financial condition and results in all material respects

  HIGH

- [ ] Certify responsibility for establishing and maintaining disclosure controls (DC&P) and ICFR

  HIGH

- [ ] Evaluate effectiveness of disclosure controls as of the end of the period (within 90 days of report date)

  HIGH

- [ ] Disclose to auditors and audit committee all significant deficiencies and material weaknesses in ICFR

  HIGH

- [ ] Disclose any fraud, whether or not material, involving management or employees with a significant role in ICFR

  HIGH

- [ ] Run a formal sub-certification process: business unit and functional leaders sign sub-certs feeding the CEO/CFO certification

  HIGH

- [ ] Maintain a Disclosure Committee charter and meet before each filing to vet draft MD&A and risk factors

SECTION 404 ICFR

- [ ] Prepare annual management report on ICFR under Section 404(a), included in Item 9A of Form 10-K

  HIGH

- [ ] State management's responsibility for establishing and maintaining adequate ICFR

  HIGH

- [ ] Identify the framework used to evaluate ICFR

  HIGH

  COSO 2013 Internal Control Integrated Framework is the standard.

- [ ] Provide management's assessment of ICFR effectiveness as of fiscal year end

  HIGH

- [ ] Disclose any material weakness identified, with description and remediation plan

  HIGH

- [ ] Accelerated and large accelerated filers: obtain external auditor attestation on ICFR under 404(b) and PCAOB AS 2201

  HIGH

- [ ] Reconcile management's ICFR conclusion with the auditor's opinion before filing
- [ ] Document scoping memo annually covering significant accounts, locations, and processes

COSO 2013 FRAMEWORK

- [ ] Adopt COSO 2013 Internal Control Integrated Framework as the basis for ICFR design and assessment

  HIGH

- [ ] Map controls to all 5 COSO components: Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring

  HIGH

- [ ] Demonstrate that all 17 COSO principles are present and functioning

  HIGH

- [ ] Document tone at the top through board minutes, code of conduct, and ethics training records
- [ ] Perform an annual fraud risk assessment covering financial reporting, asset misappropriation, and management override
- [ ] Document information and communication flows from operations to financial reporting

ICFR SCOPING

- [ ] Perform top-down, risk-based scoping per PCAOB AS 2201

  HIGH

- [ ] Identify significant accounts and disclosures based on quantitative materiality and qualitative risk factors

  HIGH

- [ ] Calculate planning materiality and tolerable misstatement with the external auditor

  HIGH

- [ ] Map significant accounts to relevant business processes (O2C, P2P, H2R, R2R, treasury, tax)

  HIGH

- [ ] Identify in-scope locations and components using a risk-based approach

  HIGH

- [ ] Identify financial reporting systems and supporting IT applications in scope for ITGCs

  HIGH

- [ ] Identify relevant assertions for each significant account (existence, completeness, valuation, rights/obligations, presentation)
- [ ] Refresh scoping annually and document changes (acquisitions, divestitures, system migrations)

ENTITY-LEVEL CONTROLS

- [ ] Document entity-level controls (ELCs) covering board oversight, code of conduct, whistleblower hotline, HR policies

  HIGH

- [ ] Operate an independent audit committee with at least one financial expert per SEC rules

  HIGH
- [ ] Maintain a whistleblower hotline under Section 301: anonymous reporting, audit committee oversight

  HIGH
- [ ] Document a Code of Ethics for senior financial officers under Section 406
- [ ] Run periodic ethics and SOX training for finance, accounting, and IT staff
- [ ] Maintain a delegation of authority (DOA) matrix with approval thresholds

ITGCS

- [ ] Document ITGCs across logical access, change management, and computer operations for each in-scope system

  HIGH
- [ ] Logical access: provisioning, deprovisioning SLA, periodic User Access Reviews (UARs), privileged access monitoring

  HIGH
- [ ] Segregation of duties within ERP roles, with SoD conflict matrix and quarterly review

  HIGH
- [ ] Change management: separate dev/test/prod, change approval, testing evidence, no developer access to production

  HIGH
- [ ] Computer operations: job scheduling, backup, incident and problem management

  HIGH
- [ ] Test ITGCs for design and operating effectiveness

  HIGH

  ITGC failure can invalidate reliance on automated application controls.
- [ ] Document and test interface controls for data flows between systems (boundary controls, reconciliations)
- [ ] Cover service organizations via SOC 1 Type 2 reports and complementary user entity controls (CUECs)

PROCESS-LEVEL CONTROLS

- [ ] Document key controls in a Risk Control Matrix (RCM) per process: risk, control, frequency, type, owner, assertion

  HIGH
- [ ] Segregate duties between preparer and approver for JEs, AP vouchers, payroll, wires

  HIGH
- [ ] Review and approve all manual journal entries above defined threshold

HIGH

Special scrutiny on top-side and consolidation entries.

- [ ] Reconcile all material balance sheet accounts monthly (bank, AR, AP, inventory, fixed assets, intercompany, accruals)

  HIGH

- [ ] Review revenue recognition controls under ASC 606 (contract, performance obligations, transaction price, allocation, recognition)

  HIGH

- [ ] Review stock-based compensation under ASC 718 (grant approval, fair value, forfeitures, expense recognition)

  HIGH

- [ ] Review lease accounting under ASC 842 (identification, classification, ROU asset and liability)

  HIGH

- [ ] Review income tax provision under ASC 740 quarterly, including uncertain tax positions and valuation allowances

  HIGH

- [ ] Approve vendor master file additions/changes with independent verification of banking details (fraud mitigation)
- [ ] Approve customer master file additions and credit limit changes
- [ ] Review accruals and estimates with documented methodology and management challenge

PERIOD-END REPORTING

- [ ] Maintain a financial close calendar with owners, dependencies, and review checkpoints

  HIGH

- [ ] Perform analytical review of P&L and balance sheet by responsible controller before close sign-off

  HIGH

- [ ] Document and review consolidation entries, FX translation, and elimination entries

  HIGH

- [ ] Tie XBRL tagging and 10-Q/10-K disclosures back to source ledger balances

  HIGH

- [ ] Run a disclosure checklist against the latest SEC rules and ASC requirements
- [ ] Operate spreadsheet (EUC) controls for material spreadsheets: version control, access, formula protection, independent review

DOCUMENTATION

- [ ] Maintain process narratives or flowcharts for each in-scope business process

  HIGH

- [ ] Maintain a current RCM for every in-scope process, refreshed annually

  HIGH

- [ ] Document IPE (information produced by entity) controls: report parameters, completeness/accuracy validation, source data evidence

HIGH

- [ ] Maintain control inventory in a GRC tool (AuditBoard, Workiva, ServiceNow GRC) with status, owner, test results
- [ ] Retain SOX evidence per company retention policy (typically 7 years, per Section 802)

TESTING AND SAMPLING

- [ ] Walk through each key control at least annually, tracing a transaction from initiation to financial reporting

  HIGH
- [ ] Test design effectiveness BEFORE operating effectiveness for every key control

  HIGH
- [ ] Apply AICPA/PCAOB sampling: 25-60 samples for daily, 25 weekly, 5 monthly, 2 quarterly, 1 annual

  HIGH
- [ ] Document tester, reviewer, date, sample population, selection method, and conclusion for each test

  HIGH
- [ ] Test IT-dependent manual controls and the supporting IPE in the same test

  HIGH
- [ ] Schedule interim and roll-forward testing to cover the full reporting period
- [ ] Apply rotation strategies only for low-risk, well-controlled areas, and only with auditor concurrence

DEFICIENCY EVALUATION

- [ ] Evaluate every control deficiency using PCAOB severity framework: control deficiency, significant deficiency, material weakness

  HIGH
- [ ] Aggregate deficiencies affecting the same account or assertion before concluding on severity

  HIGH
- [ ] Remediate identified deficiencies and re-test before year-end to support a clean ICFR opinion

  HIGH
- [ ] Disclose any material weakness in Item 9A of Form 10-K with remediation status

  HIGH
- [ ] Track all deficiencies in a centralized log: owner, severity, root cause, remediation date

SECTION 409 AND 906

- [ ] File 8-K within 4 business days of material events under Section 409 and SEC Form 8-K rules

  HIGH

- [ ] Maintain an 8-K trigger checklist covering Items 1.01 through 9.01

  HIGH

  Material agreements, departures, financial guidance changes, restatements.

- [ ] Attach Section 906 certifications signed by CEO and CFO to every periodic report

  HIGH

- [ ] Brief CEO and CFO on Section 906 criminal penalties

  HIGH

  Up to $1M/10 years for knowing certification; $5M/20 years for willful.

- [ ] Apply Section 304 clawback of executive bonuses and equity gains in the event of a restatement due to misconduct

AUDIT COORDINATION

- [ ] Align the SOX testing plan with the external auditor's reliance strategy at the start of the year

  HIGH

- [ ] Hold regular status meetings with external auditor and audit committee on scope, progress, and findings

  HIGH

- [ ] Provide the external auditor timely access to RCMs, evidence, and management's testing results to support 404(b)

  HIGH

- [ ] Manage PBC (prepared by client) list with owners and due dates
- [ ] Conduct a post-audit lessons learned with internal audit, external audit, and finance leadership