SOX Compliance Checklist

SOX compliance is never easy, but it plays an important role in assuring your organization maintains accurate financial reporting and strong internal controls. To help you maintain SOX compliance, we have put together this easy-to-follow, step-by-step checklist for navigating SOX requirements.

1 Understand SOX Requirements

Before you can comply, you need to know what you're complying with.

- [ ] **Review the key sections of SOX**
  - **Section 302:** Corporate responsibility for financial reporting
  - **Section 404:** Management assessment of internal controls
  - **Section 906:** Criminal penalties for false certifications
  - **Other relevant sections:** 401, 802, 806
- [ ] **Identify which SOX sections apply to your organization (public company, subsidiary, etc.)**

Tips & Best Practices

- **Start with a SOX applicability matrix.** Map out each section of the law to determine relevance for your business and processes.
- **Get legal and audit teams aligned early** to avoid misinterpretation of your obligations.
- **Use industry examples** to benchmark how similar organizations interpret SOX applicability.
- **Keep your compliance scope updated annually,** especially after acquisitions, IPO prep, or system overhauls.
- **Create a SOX summary guide** tailored to internal stakeholders so everyone knows what's expected.

Key Stakeholders

General Counsel
Interprets legal obligations

Chief Financial Officer (CFO)
Oversees financial reporting accountability

Internal Audit Lead
Assists in mapping controls to specific SOX sections

Compliance Officer / Risk Management Lead
Coordinates SOX scoping and applicability

2 Build Your SOX Compliance Team

SOX compliance is a team sport—get the right players on the field.

- [ ] **Appoint an internal SOX owner**

  This is typically someone from Finance, IT, or GRC who understands the cross-functional nature of SOX and can manage timelines, audits, and stakeholder coordination.

- [ ] **Involve IT, Security, HR, and Internal Audit teams**

  Each group brings a critical piece of the compliance puzzle—from access controls and change management to employee onboarding and financial integrity.

- [ ] **Define roles and responsibilities across stakeholders**

  Clarity prevents duplication, delays, and finger-pointing. Use a RACI matrix to formalize accountability (Responsible, Accountable, Consulted, Informed).

- [ ] **Align with external auditors on scope and timelines**

  Get on the same page early. Misalignment here can cause late-stage chaos.

Tips & Best Practices

- **Choose a SOX lead with cross-functional credibility,** someone who can speak "finance," "tech," and "audit" fluently.
- **Kick off with a formal team charter** that outlines the team's goals, scope, and reporting structure.
- **Hold regular syncs** (monthly or biweekly) to track progress, surface blockers, and prepare for key deadlines.
- **Loop in external audit partners early.** Don't wait until you're handing over documentation. Audit partners can flag gaps before they become findings.
- **Use project management tools** like Jira, Asana, or even a well-organized Gantt chart to track control owners, test dates, and evidence gathering.

Key Stakeholders

SOX Program Owner
Leads coordination and ensures alignment

IT & Security Leads
Own technical controls, access management, and change tracking

Internal Audit Partner
Provides oversight, testing, and readiness assessment

HR
Supports personnel-related controls (e.g., onboarding, terminations)

External Auditors
Validates controls and identifies deficiencies

3 Establish a SOX Compliance Framework

Create the structure that will guide your compliance activities.

- [ ] **Define and document internal control objectives**

  Identify what you need to protect—financial reporting accuracy, data integrity, system access, and more. Control objectives provide the "why" behind each control.

- [ ] **Map controls to SOX sections (e.g., financial reporting, access control)**

  This ensures nothing falls through the cracks and your controls align directly with compliance requirements.

- [ ] **Choose a controls framework (e.g., COSO)**

  Most organizations use COSO (Committee of Sponsoring Organizations of the Treadway Commission) for its balance of structure and flexibility.

- [ ] **Classify controls by breaking them down into the following categories**

  - **Entity-level controls:** Governance, tone at the top, risk management
  - **IT General Controls (ITGCs):** Change management, logical access, system operations
  - **Process-level controls:** Specific to workflows like payroll, procure-to-pay, or financial close

Tips & Best Practices

- **Start with what you have**—review existing policies, procedures, and audits to avoid duplicating effort.
- **Don't over-engineer.** Focus first on high-risk processes that impact financial reporting.
- **Use control matrices or GRC tools** to maintain traceability between controls, objectives, and SOX sections.
- **Keep documentation audit-ready**—your framework should be clean, version-controlled, and accessible to internal and external stakeholders.
- **Use COSO's five components** (Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring) as a checklist for completeness.

Key Stakeholders

Internal Audit Lead or Risk Manager
Leads framework development and control classification

Finance & Accounting Team
Defines financial control objectives and process-level controls

GRC or Compliance Officer
Aligns framework with COSO and maintains governance documentation

SOX Program Owner
Oversees integration and ensures stakeholder alignment

4 Identify & Document Key Processes

Know what you're controlling—and document it clearly.

- [ ] **Identify financial systems and applications in scope**

  List all ERP systems, accounting platforms, billing tools, and other applications involved in financial reporting or data that feeds into it. Don't forget integration points like APIs and third-party platforms.

- [ ] **Document business processes impacting financial reporting**

  Focus on processes such as order-to-cash, procure-to-pay, payroll, and financial close. Understand where data originates, how it flows, and where controls must exist.

- [ ] **Define ownership of each process and system**

  Assign process owners and system administrators to ensure accountability for both operations and control performance.

- [ ] **Maintain process documentation and data flow diagrams**

  Use flowcharts, swim lanes, or RACI charts to visually document how information moves through systems and teams. Keep this living documentation updated as systems or roles change.

Tips & Best Practices

- **Start with your general ledger** and work backwards—map out all systems and processes that feed into it.
- **Interview process owners** to uncover undocumented workflows or shadow systems.
- **Use standardized templates** to ensure consistency across documentation. This is especially helpful during audits.
- **Capture system dependencies** and manual versus automated controls to flag high-risk areas.
- **Version-control everything.** Auditors will want a clear history of what changed, when, and why.

Key Stakeholders

Finance Systems Owner / IT Application Owner
Identifies and documents in-scope systems

Process Owners (e.g., AP/AR leads, Payroll Manager)
Map and document business workflows

Internal Audit or SOX PMO
Oversees documentation standards and ensures completeness

GRC / Compliance Team
Maintains data flow diagrams and ensures alignment with control frameworks

External Auditors
Review and validate system/process documentation during audit cycles

5 Evaluate Control Design & Effectiveness

Well-designed controls are the foundation of SOX compliance.

- [ ] **Perform control design assessment (Are controls appropriately designed?)**

  Ask: Are the controls designed appropriately to prevent or detect errors in financial reporting? Look for clarity, alignment with risks, and whether the control is repeatable and documentable.

- [ ] **Perform control effectiveness testing (Do they work as intended?)**

  It's not enough for a control to exist—it must function as intended. Test control operation over a defined period (usually a quarter or fiscal year) to validate reliability.

- [ ] **Conduct walkthroughs and control validations**

  Work through each control from end to end with control owners and auditors. This helps confirm process understanding and ensures no steps are missed or misunderstood.

- [ ] **Identify control gaps and weaknesses**

  Where controls are missing, duplicated, or ineffective, document the issue, assign remediation owners, and track progress to closure. Gaps could stem from technology changes, new processes, or outdated documentation.

Tips & Best Practices

- **Pair control owners with auditors early.** This builds alignment and helps avoid last-minute surprises.
- **Focus on high-risk controls first,** especially those tied to financial reporting and material accounts.
- **Leverage internal audit for objectivity** in testing and validation—they bring a critical outsider's lens.
- **Automate testing where possible.** Use GRC tools or control monitoring software to reduce manual lift.
- **Create a control testing schedule** to ensure coverage and avoid testing bottlenecks near audit deadlines.

Key Stakeholders

Control Owners
Execute, document, and support testing of assigned controls

Internal Audit Team
Leads independent testing, walkthroughs, and validation

SOX Program Manager / GRC Lead
Coordinates assessment, tracks remediation, and reports progress

Finance & IT Stakeholders
Provide input on control design, help identify technical or procedural gaps

External Auditors
Review testing approach and validate effectiveness for formal SOX opinion

6 Implement Access and Identity Controls

Access controls are essential to meeting SOX security requirements.

- [ ] **Ensure least-privilege access across financial systems**

  Users should only have the access required to perform their job functions—no more, no less. Review permissions regularly and remove excess access.

- [ ] **Implement role-based access control (RBAC)**

  Group users into roles based on function and assign access at the role level. This simplifies management and helps enforce consistent, scalable permissions.

- [ ] **Enforce separation of duties (SoD)**

  No single user should control all stages of a financial transaction. Design controls to avoid conflicts of interest—e.g., separating invoice creation from approval or payments.

- [ ] **Maintain an audit trail of access changes and reviews**

  Log every access change—provisioning, role updates, deactivations. Review logs periodically to ensure controls are being followed.

- [ ] **Use automated tools for user provisioning, deprovisioning, and access reviews**

  Manual processes are error-prone and hard to scale. Automating access workflows reduces risk and ensures consistent enforcement across systems.

Tips & Best Practices

- **Run quarterly access reviews** with business owners to validate who still needs what.
- **Map financial systems to SoD conflict rules** to catch violations early.
- **Automate "joiner, mover, leaver" processes** to ensure timely provisioning and deprovisioning.
- **Integrate CIEM or IGA platforms** (like Lumos!) to centralize access visibility and automate reviews.
- **Document access policies** clearly—including how access is granted, reviewed, and revoked.

Key Stakeholders

IT Security / Identity & Access Management (IAM) Team

Implements RBAC, SoD, and access logging

System Administrators

Configure and enforce access controls in financial applications

HR

Triggers access changes based on employee status (hire, role change, termination)

Process Owners / Department Managers

Validate user access during periodic reviews

GRC / Compliance Team

Oversees access policies and ensures controls align with SOX requirements

SOX Program Owner

Coordinates access reviews and ensures proper documentation for audits

7 Monitor, Test & Update Controls

Compliance is not a one-and-done—build a repeatable rhythm.

- [ ] **Establish a control testing calendar**

  Create a quarterly or annual cadence for testing controls across business processes, IT, and financial systems. This helps prevent last-minute fire drills and keeps your SOX program audit-ready year-round.

- [ ] **Remediate control issues promptly and document fixes**

  When controls fail or gaps are identified, assign clear owners, track remediation timelines, and document corrective actions in detail. This not only satisfies audit requirements—it also strengthens your overall control environment.

- [ ] **Monitor for control exceptions or failures**

  Set up alerting and reporting to catch deviations from expected control performance. Flagging issues early allows you to address them before auditors do.

- [ ] **Regularly review and update controls as systems or risks evolve**

  Cloud migrations, org changes, and new tools can all impact controls. Build in time for periodic reviews to keep your control set aligned with current systems, roles, and business risks.

Tips & Best Practices

- **Use a shared calendar or GRC platform** to manage testing schedules and owner accountability.
- **Automate exception reporting** wherever possible—look for anomalies in access logs, usage, or control performance.
- **Log remediation efforts in your SOX repository** with timestamps, owners, and root cause notes for audit traceability.
- **Schedule "SOX retrospectives"** post-audit to identify improvement areas and reset priorities for the next cycle.
- **Use risk assessments** to drive control updates—not just changes in tools or org structure.

Key Stakeholders

Internal Audit
Owns testing calendar, performs control evaluations, and tracks exceptions

Control Owners
Monitor their respective controls and address failures or breakdowns

SOX Program Manager / GRC Lead
Coordinates testing, facilitates remediation tracking, and updates documentation

IT & Finance Teams
Support testing cycles, assist with fixes, and validate that updated controls are operational

Executive Stakeholders / Audit Committee
Review program performance and prioritize resources for remediation when needed

8 Prepare for the SOX Audit

Get your house in order before the auditors knock.

- [ ] **Define the scope and objectives of the audit**

  Clarify which entities, systems, processes, and controls are in scope. This avoids scope creep and ensures everyone is focused on what matters most.

- [ ] **Gather and organize required documentation and evidence**

  Compile control descriptions, testing results, access logs, policies, and process documentation in one centralized, well-structured repository.

- [ ] **Conduct mock audits or readiness assessments**

  Internal audit or a third party can run a dry run of the audit to surface gaps before external auditors. This is especially useful for first-time SOX programs or after major system changes.

- [ ] **Address auditor questions and requests in a timely manner**

  Have a process in place to respond to document requests, clarifications, or walkthroughs. Delays here can hurt audit timelines—and confidence.

- [ ] **Track and resolve any findings or deficiencies**

  Log any issues raised by auditors, assign owners, and monitor remediation to closure. This shows continuous improvement and helps prevent repeat findings.

Tips & Best Practices

- **Create a shared audit binder** (physical or digital) organized by SOX section or control domain to simplify handoffs.
- **Schedule a pre-audit kickoff meeting** with all stakeholders—including auditors—to set expectations and timelines.
- **Use a response tracker** to manage auditor requests and avoid duplicate efforts or missed deadlines.
- **Assign a single point of contact (SPOC)** to manage communications between your team and the auditors.
- **Document the remediation process** thoroughly, including root cause and resolution date—auditors love a good paper trail.

Key Stakeholders

SOX Program Manager / GRC Lead

Coordinates audit scope, readiness, and communications

Internal Audit

Conducts mock audits and ensures audit preparedness

Control Owners & Process Owners

Provide documentation and participate in walkthroughs

Finance & IT Leads

Assist with evidence collection and respond to system- or process-specific inquiries

External Auditors

Evaluate controls and issue findings or recommendations

Executive Stakeholders

Review final reports and approve remediation plans where needed

9 Maintain Ongoing Compliance

SOX isn't just an annual event—it's an ongoing discipline.

- [ ] **Automate recurring access reviews and certifications**

  Schedule regular (e.g., quarterly) reviews for user access, especially to financial systems. Automate where possible to reduce manual effort and avoid lapses.

- [ ] **Monitor high-risk access continuously**

  Focus on privileged accounts and users with elevated permissions. Use tools that can alert on suspicious behavior or policy violations in real time.

- [ ] **Train employees on SOX policies and controls**

  From system users to approvers, everyone should understand how their actions impact compliance. Make training ongoing—not just part of onboarding.

- [ ] **Revisit the compliance program quarterly or biannually**

  Update control documentation, review risk assessments, and validate that controls still align with current systems and processes.

- [ ] **Ensure new systems or vendors meet compliance standards**

  Before onboarding any new SaaS tool, system, or vendor, evaluate its impact on financial reporting and whether it aligns with SOX controls.

Tips & Best Practices

- **Automate email reminders and certifications** for access reviews—it's low effort with high impact.
- **Tag high-risk users and systems** in your identity governance or SIEM platforms for continuous monitoring.
- **Maintain a SOX change log** to track updates to systems, processes, and controls throughout the year.
- **Create a vendor onboarding checklist** that includes SOX compliance criteria—avoid surprises later.
- **Make SOX training part of company-wide security awareness efforts,** not just a niche requirement for finance.

Key Stakeholders

SOX Program Owner / GRC Lead
Oversees program cadence, owns training initiatives, and coordinates ongoing reviews

IT Security / IAM Team
Manages continuous access monitoring and automated reviews

Finance & Accounting Leaders
Ensure new systems and processes align with SOX reporting standards

Procurement / Vendor Management
Verifies third-party compliance and risk assessments before onboarding

HR & Training Team
Delivers ongoing SOX and internal control training to relevant personnel

Internal Audit
Performs periodic health checks of the SOX program and control environment

10 Leverage Technology to Scale Compliance

Manual SOX processes break at scale—automation helps fix that.

- [ ] **Implement identity and access management tools**

  Identity and access management (IAM) platforms streamline user provisioning, deprovisioning, and access reviews—key pain points in SOX compliance. Look for tools with robust audit logs, RBAC support, and integration with key systems.

- [ ] **Use automated SOX reporting and monitoring platforms**

  GRC tools and cloud-native platforms can automate control monitoring, generate audit-ready reports, and reduce time spent on evidence collection and manual testing.

- [ ] **Centralize audit evidence and documentation**

  Housing everything in a centralized, version-controlled repository reduces confusion, missed files, and last-minute scrambles before audits.

- [ ] **Track and report metrics (e.g., review completion rates, remediation times, SoD violations)**

  - Review completion rates
  - Remediation turnaround time
  - SoD violations
  - Control testing success rates

  These KPIs help you demonstrate program effectiveness and surface gaps early.

- [ ] **Integrate with ITSM and ticketing tools for end-to-end visibility**

  Link access requests, control changes, and incidents to service tickets for traceability and accountability across systems and teams.

Tips & Best Practices

- **Start with the riskiest, most time-consuming processes** —access reviews and evidence collection are great early wins for automation.
- **Choose tools that integrate easily** with your existing stack (e.g., HRIS, ticketing, cloud infrastructure).
- **Use dashboards to visualize compliance health** in real-time and drive cross-functional transparency.
- **Automate notifications and escalations** to keep reviews and remediations on track.
- **Avoid siloed tooling**—CIEM and IGA platforms like Lumos can serve as the connective layer between IAM, GRC, and ITSM.

Key Stakeholders

IT Security / IAM Team
Implements automation for access management and control enforcement

GRC or SOX Program Manager
Leads tool selection, defines compliance metrics, and oversees reporting

Internal Audit
Validates the effectiveness of automated controls and evidence logs

IT Operations / DevOps
Supports integrations with ITSM, ticketing systems, and infrastructure monitoring tools

Engineering & System Owners
Ensure new systems or processes are designed with automation hooks for compliance

Vendor Management / Procurement
Evaluates automation tools for compliance and system compatibility

FINAL TIP

Be Audit-Ready, Always with Lumos

SOX compliance shouldn't be a once-a-year scramble. The most resilient organizations treat it as an always-on discipline—powered by clear controls, automated processes, and continuous visibility. That's where Lumos comes in.

Lumos is the first autonomous identity platform that helps organizations stay SOX-compliant without drowning in manual effort. By unifying identity governance, access reviews, privileged access management, and lifecycle automation into one streamlined platform, Lumos gives IT and security teams full control over who has access to what—across every app, system, and identity type.

With Lumos, you can automatically enforce least-privilege access, detect risky or excessive permissions, and generate audit-ready reports with just a few clicks. No more spreadsheet chaos. No more last-minute evidence collection. Just real-time insights and automated workflows that make continuous compliance not only possible—but painless.

Whether you're preparing for your first SOX audit or looking to scale your program across hundreds of systems, Lumos helps you eliminate blind spots, reduce risk, and prove compliance every single day.

Want to see how Lumos simplifies SOX compliance?

Take the first step toward always-on audit readiness.

Book a demo today