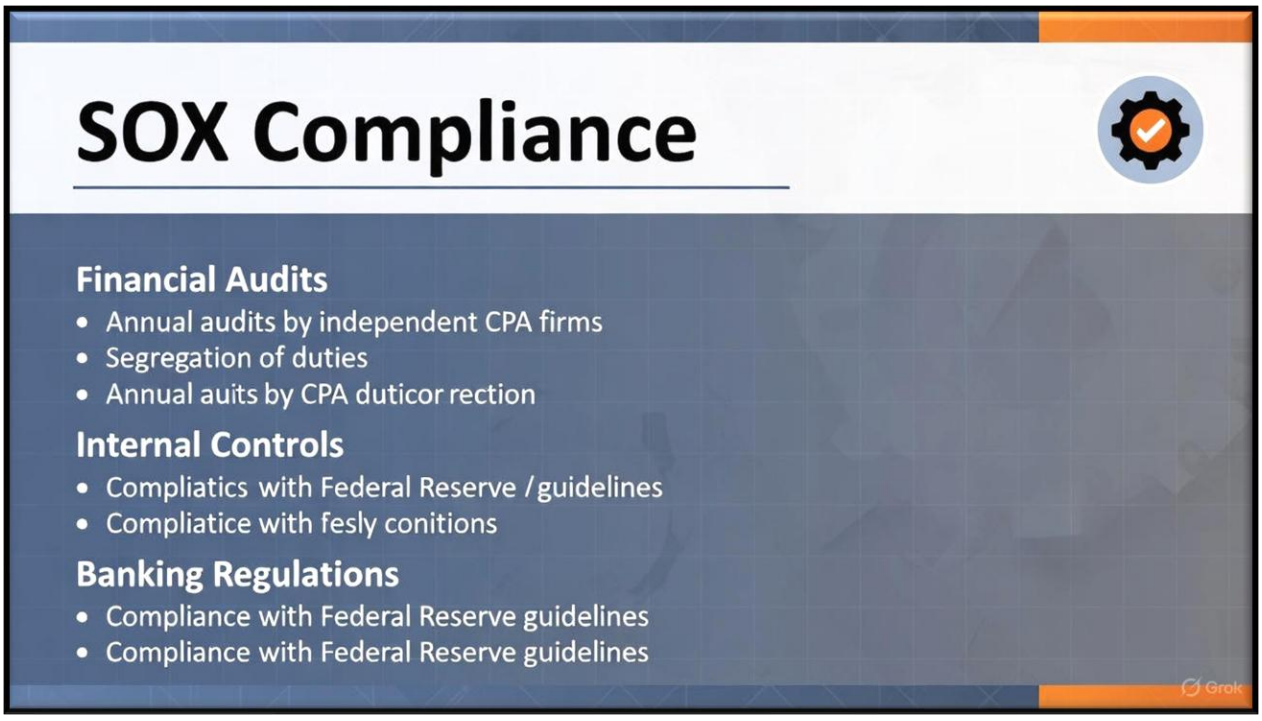


Thomas Bronack, CBCP

bronackt@gmail.com | (917) 673-6992

Table of Contents

Contents

Executive Summary: Sarbanes-Oxley Act (SOX)

History, Importance, Benefits, and Consequences of Non-Compliance

History & Purpose

Enacted in July 2002 in direct response to major corporate accounting scandals (Enron, WorldCom, Tyco, Adelphia), the Sarbanes-Oxley Act represents the most significant reform of U.S. securities laws since the 1930s. Sponsored by Senator Paul Sarbanes and Representative Michael Oxley, SOX was designed to restore public trust in capital markets by strengthening corporate governance, enhancing the accuracy and reliability of financial reporting, and imposing strict accountability on senior executives and auditors of publicly traded companies.

Strategic Importance for Large Banking Organizations

For publicly traded banks, SOX compliance is not merely a regulatory obligation—it is a cornerstone of enterprise risk management. Sections 302, 404(a), and 404(b) mandate rigorous internal control over financial reporting (ICFR), independent auditor attestation, and personal CEO/CFO certification of financial statements. In the highly regulated banking sector, effective SOX controls directly support compliance with Basel III, CECL/ALLL, FDICIA (for institutions > $500M in assets), and broader regulatory expectations from the OCC, Federal Reserve, and FDIC.

Key Benefits of Sustained SOX Adherence

- Enhanced investor confidence and lower cost of capital (empirical studies show SOX-compliant firms enjoy 50–150 bps lower borrowing spreads).
- Early detection and prevention of financial misstatements and fraud through robust ICFR.
- Strengthening corporate governance and tone-at-the-top culture.
- Operational efficiencies from standardized, automated controls (especially ITGCs and process-level controls).
- Competitive advantage in mergers, acquisitions, and capital markets transactions (clean SOX 404 opinions are scrutinized by rating agencies and institutional investors).
- Reduced regulatory scrutiny and examination findings from banking supervisors.

Penalties and Consequences of Non-Compliance

SOX violations carry severe civil and criminal penalties:

- Material Weakness or Adverse Opinion: Immediate stock price decline (average 2–10% drop upon disclosure), increased cost of capital, heightened regulatory intervention, and potential delisting proceedings
- Section 302/906 False Certification: – Civil penalties up to $5 million – Criminal penalties up to 20 years imprisonment for willful violations
- Section 1102 Tampering with Records: Up to 20 years imprisonment

- SEC enforcement actions, disgorgement of bonuses and profits (claw-back under Section 304), and officer/director bars
- Reputational damage and loss of customer/investor trust (often irreversible in banking)
- Class-action shareholder lawsuits and derivative suits against directors and officers

Conclusion Twenty-three years after its passage, SOX remains the gold standard for financial reporting integrity in U.S. public companies. For large banking institutions, sustained investment in SOX-compliant internal controls is not a cost center but a strategic imperative that protects franchise value, satisfies multiple regulators simultaneously, and directly contributes to long-term shareholder value. Non-compliance is simply not an option in today's enforcement and transparency environment.

Maintaining an unqualified SOX 404(b) attestation is one of the clearest signals a public bank can send that its financial reporting, risk management, and governance processes are robust, reliable, and worthy of investor and regulator confidence.

Sarbanes Oxley pertinent sections and their meaning

Section 302 – Corporate Responsibility for Financial Reports

Requirement CEO and CFO must personally certify in each quarterly (10-Q) and annual (10-K) filing that:

- They have reviewed the report
- It does not contain untrue statements or omit material facts
- Financial statements accurately present in all material respects the financial condition and results of operations
- They are responsible for establishing and maintaining ICFR and disclosure controls and procedures (DC&P)
- They have evaluated the effectiveness of DC&P within 90 days and presented their conclusions
- They have disclosed to the auditors and audit committee all significant deficiencies, material weaknesses, and any fraud involving management or employees with a significant role in ICFR

Typical Compliance Evidence Leading to Clean Attestation

- Signed Sub-section 302 certification documents for every filing in the period under audit
- Documented quarterly "bring-down" disclosure committee meetings with minutes
- Evidence of CEO/CFO disclosure of any significant deficiencies or fraud to the auditor and audit committee (none in a clean year)
- Disclosure controls checklist signed off each quarter

Section 404 – Management Assessment of Internal Controls

Consists of two parts:

Section 404(a) – Management's Annual Report on ICFR

Management must state its responsibility for ICFR and provide an assessment of effectiveness as of year-end.

Section 404(b) – Auditor Attestation

(applies to large accelerated and accelerated filers, including virtually all large banks)

The external auditor must attest to and report on management's assessment (integrated audit).

Framework Used Almost universally the 2013 COSO Internal Control – Integrated Framework (the five components: Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring Activities).

Key Audit Procedures and Evidence for Unqualified Opinion

- Scoping using the SEC/PCAOB "top-down, risk-based" approach: – Identify significant accounts and disclosures (e.g., loan loss reserves, ALLL/ACL, fair value of Level 3 instruments, interest income, deposits, derivatives, etc.) – Identify entity-level controls (ELCs), IT general controls (ITGCs), and process-level controls that are material – Heavy reliance on banking-specific cycles: credit, treasury, deposits, lending, payments, GL
- Walkthroughs of all in-scope processes (lending/credit loss provisioning, deposit operations, investment securities, derivatives, etc.)
- Testing of operating effectiveness of key controls: – Entity-level: tone-at-the-top interviews, code of conduct acknowledgments, whistleblower log review, fraud risk assessment – ITGCs: change management, logical access, computer operations (especially critical for core banking systems such as FIS, Fiserv, Jack Henry, Temenos, etc.) – Process-level: loan review, ALLL/CECL model governance and validation, interest rate risk modeling, BSA/AML monitoring, reconciliation controls, manual journal entry reviews, etc.
- Deficiency evaluation using both quantitative and qualitative factors (PCAOB AS 2201 and SEC interpretive guidance)
- No material weaknesses identified → management conclusion "effective" and auditor unqualified opinion

Section 906 – Criminal Penalties for Certification (18 U.S.C. § 1350)

CEO/CFO written certification accompanying each periodic report that the report fully complies with the Exchange Act and information is fairly presented. Willful violation can carry 20-year felony penalties.

Evidence Separate 906 certification filed as Exhibit 31/32 with every 10-K and 10-Q (auditor re-performs review of filing).

Section 301 & 406 – Audit Committee & Code of Ethics

- Audit committee financial expert, independence, direct responsibility for appointing/retaining auditor

- Disclosure of whether the bank has a written Code of Ethics for senior financial officers (or why not)

Evidence Audit committee charter, pre-approval policies, minutes showing direct communication with auditor, Form 10-K Item 9A disclosures, published Code of Ethics on website.

Section 402 – Enhanced Conflict of Interest Provisions

Prohibits personal loans to directors and executive officers (very important for banks).

Evidence Annual D&O questionnaire confirming no prohibited loans/extensions of credit in violation of Reg O and SOX 402.

Outcome of a Successful Third-Party Attestation

(Clean SOX 404(b) Report)

The auditor issues an integrated audit report that contains two opinions:

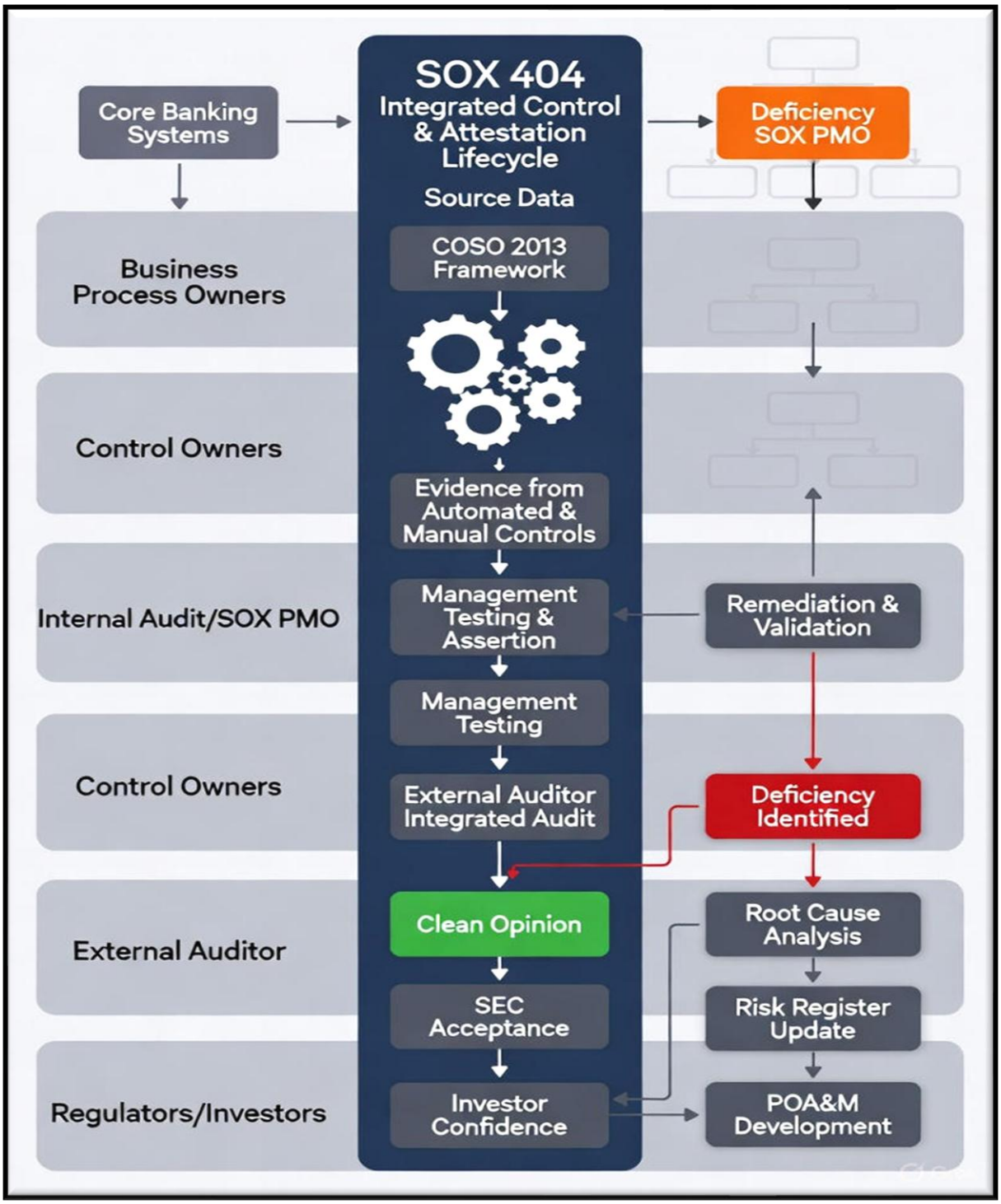
1. Unqualified opinion on the fairness of the financial statements
2. Unqualified opinion that the banking organization maintained, in all material respects, effective internal control over financial reporting as of [year-end date], based on COSO 2013 criteria.

Typical wording in the 10-K: “We did not identify any material weaknesses in our internal control over financial reporting… XYZ LLP (the independent registered public accounting firm) has issued an attestation report on our internal control over financial reporting which appears on the following page…”

This combination of evidence and testing, with no material weaknesses identified, is what leads to a clean SOX attestation for a large banking organization.

SOX Integrated Control & Attestation Ecosystem

in a Large Banking Organization (Visual Concept for Executive Presentation)



"SOX 404 Integrated Control & Attestation Lifecycle"

Diagram provides, Horizontal swim-lanes showing the key owners:

- Business Process Owners,
- Control Owners,
- Internal Audit/SOX PMO,
- External Auditor, and
- Regulators/Investors.

Visual Flow (Top → Bottom)

1. **Source Data & Transaction Layer** (Bottom of diagram) Icons: Core banking system (FIS/Fiserv/Temenos), loan origination, treasury workstations, payment rails, general ledger → Data feeds into automated and manual controls
2. **Control Environment (COSO 2013 Framework)** Five interlocking gears surrounding the central flow:
    - Control Environment (Tone at the Top) and Risk Appetite
    - Risk Assessment (Annual SOX Scoping & Risk Register)
    - Control Activities (ITGCs + Automated + Manual Controls)
    - Information & Communication
    - Monitoring Activities

    Each gear shows key banking examples:

    - CECL/ALLL model governance
    - Change management & access controls
    - Reconciliations, journal entry reviews, IPE
3. Information Production & Evidence Gathering Central arrow upward labeled "Evidence Flow"
    - Automated evidence from GRC tool (Archer, ServiceNow, MetricStream)
    - Quarterly control performance testing by process owners
    - SOX PMO centralized evidence repository
    - Deficiency tracking via **Risk Register** and **POA&M (Plan of Action & Milestones)**
4. Management Testing & Assertion (Section 404(a)) Icon: Management sign-off dashboard
    - Q1–Q3 roll-forward testing
    - Year-end 302/906 sub-certifications cascade (business unit → CFO/CEO)
    - Management's conclusion: "ICFR Effective – No Material Weaknesses"
5. External Auditor Integrated Audit (Section 404(b)) Icon: Big-4 audit firm logo + PCAOB AS 2201
    - Auditor re-performance of management testing on key controls
    - Walkthroughs, deficiency evaluation, materiality scoping
    - Dual-purpose testing (substantive + controls)
6. Decision Point – Clean vs. Rejection Loop Large diamond in the center: "Unqualified Opinion?"

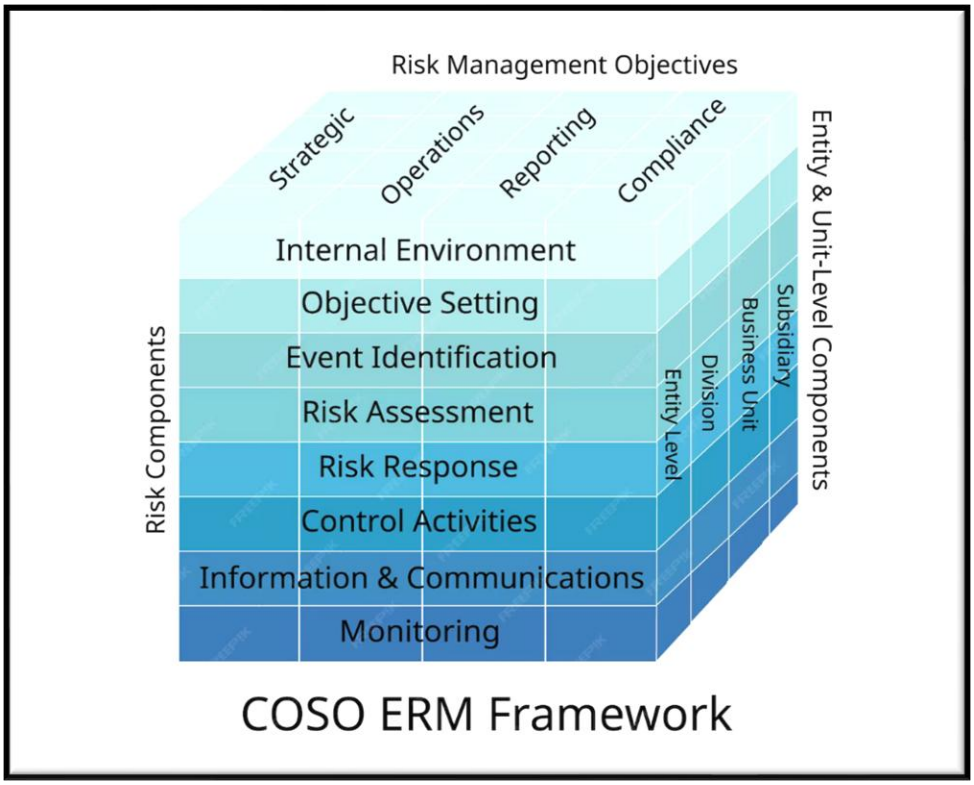
Green Path (Success → Right Side) → Unqualified ICFR opinion + Unqualified financial statement opinion → Filed with 10-K (Item 8 & 9A) → Accepted by SEC, Federal Reserve, OCC, FDIC, rating agencies, institutional investors → Stock price stability / lower cost of capital

Red Path (Rejection / Adverse → Left Side Feedback Loop) → Significant Deficiency or Material Weakness identified → Immediate disclosure via 8-K Item 4.02 (if material weakness) → Entry into **Risk Register** (centralized tracking) → Mandatory **POA&M** created with: – Root cause analysis – Remediation owner & target date – Compensating controls (if needed) – Quarterly status updates to Audit Committee → Re-testing by Internal Audit & External Auditor in next cycle → Loop continues until resolved → feeds back into main flow

7. **Top of Diagram – Final Acceptance** Icons: SEC EDGAR stamp, clean 10-K, investor confidence meter (green), regulator "no findings" checkmark

This single-page visual clearly communicates to the Board, Audit Committee, and regulators how SOX is not a siloed exercise but an enterprise-integrated discipline with built-in feedback loops that drive continuous improvement and ultimately deliver the required unqualified third-party attestation.

COSO and its relevance to SOX Attestation Reviews



Summary of COSO: History, Structure, and Critical Importance in SOX Attestation

Aspect	Details
Full Name	Committee of Sponsoring Organizations of the Treadway Commission
Founded	1985
Sponsoring Organizations	AAA, AICPA, FEI, IIA, IMA (five major U.S. professional associations)
Original Purpose (1985)	To study the causes of fraudulent financial reporting (Treadway Commission) and sponsor solutions
Current Role	De-facto standard-setter for internal control frameworks in the U.S. and globally

Key COSO Publications & Evolution

Year	Publication	Significance for SOX
1992	Internal Control – Integrated Framework (the original "1992 Framework" or "Cube")	First comprehensive internal control model
2004	Enterprise Risk Management – Integrated Framework (ERM)	Expanded the cube into risk management
2006	Guidance for Smaller Public Companies	Practical application tips for non-large filers
2009	Guidance on Monitoring Internal Control Systems	How to satisfy the monitoring component
2013	Internal Control – Integrated Framework (updated) + Illustrative Tools	The version currently required by the SEC for SOX compliance
2017	Enterprise Risk Management – Integrating with Strategy and Performance	Updated ERM (not required for SOX)

The COSO 2013 Framework – The 5 Components (the "Cube")

Component	Description	SOX Relevance
1. Control Environment	Tone at the top, ethics, governance, structure, HR standards	Foundation – weakness here often = material weakness
2. Risk Assessment	Identify & analyze risks to financial reporting objectives	Drives scoping of significant accounts and processes

3. Control Activities	Policies & procedures (preventive & detective, manual & automated, ITGCs & application controls)	Where most SOX key controls live
4. Information & Communication	Capture and share information needed for controls (internal & external)	Supports evidence retention and financial close
5. Monitoring Activities	Ongoing evaluations & separate evaluations (internal audit, self-assessment)	Required to conclude controls operate over time

17 Principles and Points of Focus

The 2013 Framework introduced **17 principles** (3–5 per component) that must all be "present and functioning" for ICFR to be effective. Examples:

- Principle 1: Demonstrates commitment to integrity and ethical values
- Principle 12: Deploys control activities through policies and procedures
- Principle 16: Performs ongoing and/or separate evaluations

Auditors explicitly evaluate and document each of the 17 principles in every SOX 404 audit.

Why COSO Is Essential for SOX Attestation

Requirement	How COSO Satisfies It
SEC Rule (2003 & later)	Explicitly states that management must base its SOX 404(a) assessment on a "suitable, recognized control framework" and names COSO as an example that meets the criteria
PCAOB AS 2201	Requires the auditor to use the same framework as management (almost always COSO 2013 in the U.S.)
Management Report (10-K)	Must state that ICFR is designed and assessed using the COSO 2013 Framework
Auditor's Attestation (404(b))	Auditor opines whether management's assessment using COSO is fairly stated and whether ICFR is effective under COSO criteria
Material Weakness Definition	A material weakness exists when one or more of the five components is not present and functioning (or one or more of the 17 principles has a major deficiency)

Practical Impact on a SOX 404 Audit

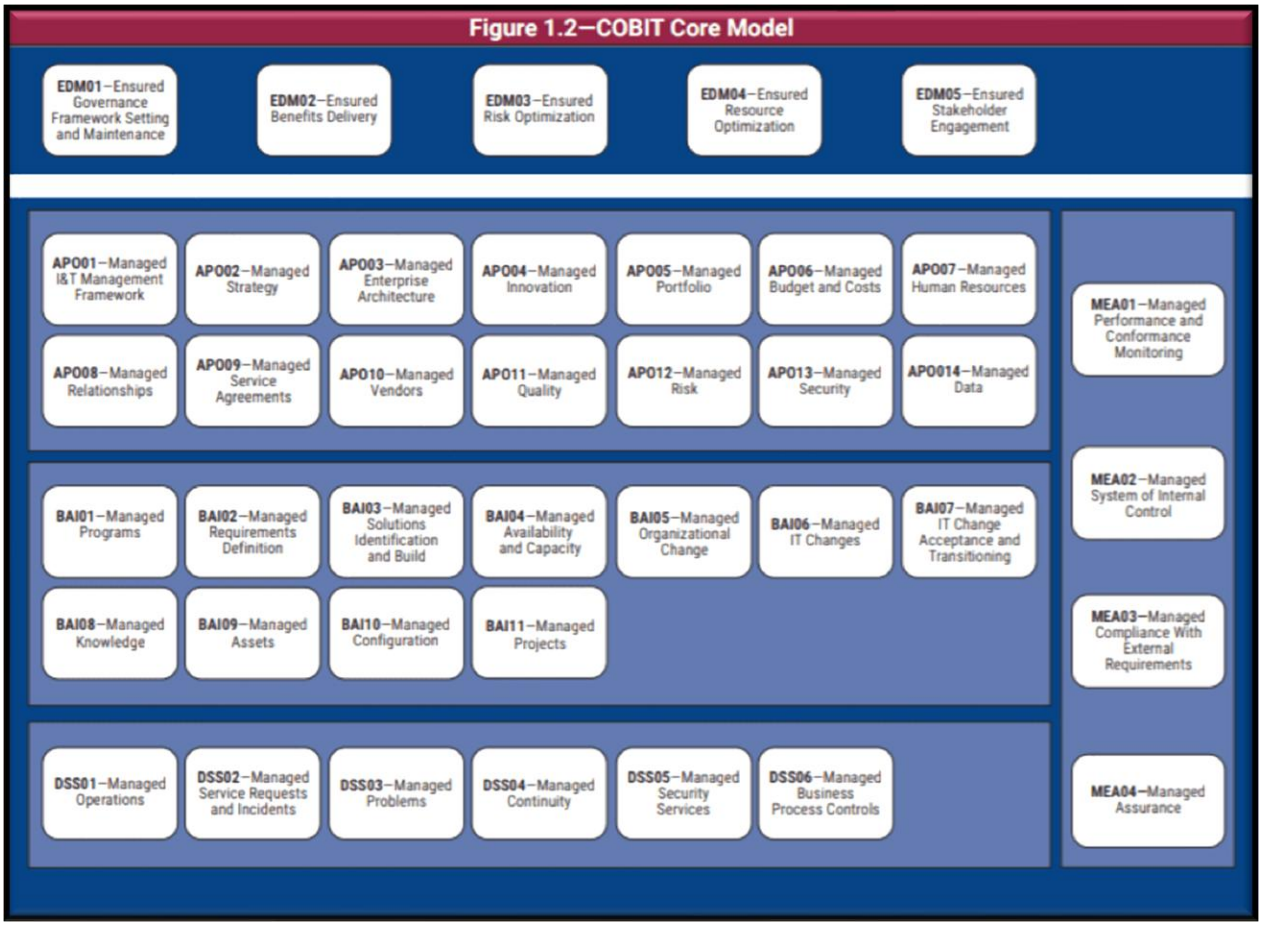
- **Scoping** → performed using COSO's risk assessment principles
- **Documentation** → organized around the 5 components and 17 principles
- **Testing** → evaluates whether controls satisfy the relevant points of focus
- **Deficiency evaluation** → explicitly mapped to which component(s)/principle(s) are deficient
- **Management's conclusion & auditor opinion** → both reference COSO 2013

Bottom Line

COSO 2013 is **the required framework** for virtually every U.S. public company performing a SOX 404 attestation. If a company claims its ICFR is effective, it is effectively stating: "All 5 COSO components are present and functioning, and all 17 principles are present and functioning with no major deficiencies."

Using any other framework (or no framework) is technically possible but almost never accepted by the SEC or external auditors. COSO 2013 is the universal language of SOX compliance in the United States.

COBIT Framework



Overview of COBIT Core Model (COBIT 2019)

COBIT (Control Objectives for Information and Related Technologies) is the leading IT governance and management framework developed by ISACA. The current version is COBIT 2019.

Component	Description	Number
Governance and Management Objectives	5 Governance objectives + 35 Management objectives that cover all enterprise IT activities	40

Design Factors	Factors used to tailor the framework (e.g., company size, risk profile, IT deployment model)	11
Focus Areas	Optional toolkits for specific topics (e.g., DevOps, Cloud, Small & Medium Enterprises, Cybersecurity)	–
Components of a Governance System	The 7 enablers that make governance work:	7
	1. Principles, Policies & Frameworks	
	2. Processes (the 40 objectives)	
	3. Organizational Structures	
	4. Information Flows & Items	
	5. Culture, Ethics & Behavior	
	6. People, Skills & Competencies	
	7. Services, Infrastructure & Applications	
Capability Levels (Maturity)	0–5 scale (0 = Incomplete → 5 = Optimizing) for each process	6 levels
Process Reference Model	Each of the 40 objectives contains detailed guidance: purpose, alignment goals, process practices (APO01–DSS06 naming convention)	

The 5 Domains in COBIT 2019

Domain	Code	Focus Area	Example Objectives
1. Evaluation, Direct and Monitor	EDM	Governance direction & oversight	EDM01, EDM03
2. Align, Plan and Organize	APO	Strategy, architecture, HR, portfolio	APO01–APO13
3. Build, Acquire and Implement	BAI	Solutions delivery, change management	BAI01–BAI11
4. Delivery, Services and Support	DSS	Operations, service desk, security services	DSS01–DSS06
5. Monitor, Evaluate and Assess	MEA	Performance, compliance, assurance	MEA01–MEA03

Why COBIT Directly Pertains to SOX Attestation Reviews

SOX Section 404 requires management and auditors to assess the effectiveness of Internal Control over Financial Reporting (ICFR). A very large portion of material is financial statement balances and disclosures today originate from or flows through IT systems (ERP, revenue systems, etc.). Therefore, IT-dependent controls and IT General Controls (ITGCs) are almost always in scope.

Direct Linkages Between COBIT and SOX ITGC Testing

SOX ITGC Domain (Typical)	Primary COBIT 2019 Objectives Tested in SOX	Relevance to Financial Reporting
Logical Access (user provisioning, terminations, privileged access, periodic review)	APO01 (Managed IT Management Framework), APO07 (Managed Human Resources), DSS05 (Managed Security Services), DSS06 (Managed Business Process Controls)	Prevents unauthorized changes or transactions that could cause material misstatement
Change Management (program changes, migrations, emergency changes)	BAI06 (Manage Changes), BAI10 (Manage Configuration)	Ensures changes to financial applications are authorized, tested, and do not introduce errors
Computer Operations (job scheduling, backups, incident management)	DSS01 (Manage Operations), DSS02 (Manage Service Requests and Incidents), DSS03 (Manage Problems)	Ensures completeness and accuracy of automated processing and availability of data
Systems Development Life Cycle (SDLC) (for new systems or major upgrades)	BAI01–BAI04 (program/project management, requirements, solution delivery)	Ensures new financial systems are properly designed and implemented

Practical Use in SOX Programs

How Companies/Auditors Use COBIT for SOX

- **Mapping:** Most Big-4 and large public companies explicitly map their SOX ITGC controls to COBIT objectives (e.g., “Change Management – BAI06.01”).
- **Risk & Control Matrices (RCMs):** COBIT process practices are frequently used as the source of control objectives and suggested controls.
- **Scoping:** If a COBIT domain/objective is deemed high-risk and in-scope for financial reporting, all related applications are usually included.
- **Deficiency Evaluation:** Failure of a key COBIT control (especially in DSS05, BAI06, APO07) frequently leads to at least a significant deficiency, sometimes a material weakness.
- **Remediation:** Companies often adopt COBIT language and capability maturity targets when remediating ITGC findings cited by external auditors.

Summary: Why COBIT Is Critical to SOX

1. **COSO 2013** (the primary framework for ICFR) explicitly states that IT general controls are part of the control activities and information & communication components.
2. **PCAOB AS 2201** requires auditors to test ITGCs when the company relies on automated controls or IT-dependent manual controls.
3. **COBIT 2019** is the de-facto global standard for defining, documenting, and assessing IT general controls.
4. Using **COBIT** ensures consistency, completeness, and auditability of the IT control environment that supports reliable financial reporting — the core objective of SOX 404.

In short, while COSO is the overarching ICFR framework required by the SEC, COBIT is the most widely adopted and auditor-accepted framework for the IT portion of SOX 404 attestation reviews.

Steps to Complete a SOX Attestation Audit (Section 404)

Typical Timeline (Dec 31 year-end example)

This sequence is followed every year for U.S. public companies subject to SOX 404(b). Non-accelerated filers skip the external auditor's attestation (Step 13–14 on ICFR only) but still perform Steps 1–12 internally.

Seq	Phase	Step	Primary Owner	Key Deliverables / Outcome
1	Planning & Scoping	Determine in-scope accounts, locations, processes & systems (top-down risk-based scoping)	Management + Auditor	Scoping document, significant accounts list
2	Planning & Scoping	Perform entity-level controls (ELC) & fraud risk assessment	Management + Auditor	Risk assessment memo, fraud discussion with audit committee
3	Documentation	Update/create narratives, flowcharts, and risk-control matrices (RCMs) for all in-scope processes	Management (auditor reviews)	Complete SOX documentation library
4	Testing – Design	Perform walkthroughs and evaluate design effectiveness of key controls	Management + Auditor	Documented walkthroughs, design conclusions
5	Testing – Operating	Management performs ongoing testing of	Management	Management testing evidence & results

		operating effectiveness (throughout the year)		
6	Testing – Operating	Auditor performs independent testing of design & operating effectiveness (interim + year-end)	External Auditor	Auditor workpapers, testing conclusions
7	Testing – Operating	Test IT general controls (ITGCs) – access, change management, operations	Management + Auditor	ITGC testing results
8	Deficiency Evaluation	Identify, document, and aggregate control deficiencies	Management + Auditor	Deficiency log
9	Deficiency Evaluation	Classify deficiencies (control deficiency → significant deficiency → material weakness)	Management + Auditor	Final severity classification
10	Remediation (if needed)	Remediate any significant deficiencies or material weaknesses	Management	Remediation plans & evidence
11	Remediation (if needed)	Re-test remediated controls for sufficient period of operation	Management + Auditor	Re-testing evidence
12	Conclusion & Reporting	Management concludes on effectiveness of ICFR and drafts 404(a) report	Management	Management's report ("effective" or "one or more material weaknesses")
13	Conclusion & Reporting	Auditor issues integrated audit opinion: (1) Opinion on financial statements (2) Opinion on ICFR effectiveness (404(b))	External Auditor	Unqualified, Adverse, or (rarely) Disclaimer opinion on ICFR
14	Filing	File Form 10-K with SEC (includes management report + auditor's attestation report)	Management	SEC filing completed by deadline

Quarterly SOX Reviews

Quarter	Main Activities
Q1–Q2	Steps 1–5 (scoping, documentation, management testing)
Q3	Step 6 (auditor interim testing)
Q4	Year-end substantive testing + final ICFR testing
Jan–Feb (next year)	Steps 8–14 (deficiency eval, remediation, roll-forward testing, sign & file)

Narrative of steps needed for SOX Attestation Review

A SOX (Sarbanes-Oxley Act) attestation audit under Section 404 typically consists of two integrated opinions issued by the external auditor:

- **Section 404(a)**: Management's assessment of Internal Control over Financial Reporting (ICFR)
- **Section 404(b)**: Auditor's attestation (opinion) on the effectiveness of ICFR

  (For non-accelerated and some emerging growth companies, 404(b) is currently exempt, but 404(a) is still required.)

The overall process is annual and follows the PCAOB's Auditing Standard 2201 (AS 2201, formerly AS 5) for public companies in the U.S. Below are the typical high-level steps performed jointly by management and the external auditor.

Phase 1: Planning and Scoping (Both Management and Auditor)

1. Determine scope
   - Identify significant accounts, disclosures, and locations/business units.
   - Identify relevant financial statement assertions (existence, completeness, valuation, etc.).
   - Determine "in-scope" processes, systems, and controls using a top-down, risk-based approach (materiality + likelihood of misstatement).
2. Perform entity-level control (ELC) assessment
   - Evaluate control of environment, risk assessment, monitoring, IT general controls (ITGCs), period-end financial reporting controls, etc.
3. Conduct fraud risk assessment and discuss with the audit committee
   - Identify risks of management override and revenue recognition risks (AS 2401).
4. Document the scoping decisions and obtain management/audit committee approval

Phase 2: Documentation of Controls (Primarily Management, Reviewed by Auditor)

5. Update or create process narratives, flowcharts, and risk-control matrices (RCMs)
   - Document key controls (preventive/detective, manual/automated) at the process and transaction level for all in-scope processes (e.g., revenue, procurement, payroll, treasury, financial close, ITGCs).

Phase 3: Testing of Design and Operating Effectiveness

6. Test design effectiveness (both management and auditor)
   - Walkthroughs (one per key control) to confirm understanding and that controls are properly designed.
   - Test operating effectiveness
   - Management performs its own testing throughout the year (usually Q1–Q3).

- External auditor performs independent testing (typically Q3–year-end and roll-forward in Q1 of next year).

7. Testing approaches: ◦
   - Key controls → sample sizes per PCAOB guidelines (usually 1 if automated and no changes, 25–40 for manual). ◦
   - Non-key/redundant controls may be tested on a rotational basis.
8. Test IT general controls (ITGCs)
   - Access controls, change management, computer operations, and logical security over in-scope applications (e.g., ERP).

Phase 4: Evaluation of Deficiencies

9. Identify and aggregate control deficiencies
   - Classify each deficiency:
     - Control deficiency
     - Significant deficiency
     - Material weakness
   - Use both qualitative and quantitative factors (PCAOB AS 2201 and SEC guidance).
10. Perform compensatory control evaluation
    - Determine whether other controls compensate for identified deficiencies.
11. Conclude on the severity
    - A material weakness means there is a reasonable chance that a significant error could go unnoticed or not be corrected.
    - Management and auditors must agree on the classification (disagreements are rare but escalate to audit committee).

Phase 5: Remediation (If Needed)

12. Address any deficiencies prior to year-end, or at the earliest opportunity.
    - Re-test remediated controls (auditor must obtain evidence that the control operated effectively for a sufficient period).

Phase 6: Reporting

13. Management completes its 404(a) assessment
    - Draft management's report on ICFR (included in Form 10-K).
    - Conclude: "effective" or "ineffective" (one or more material weaknesses).
14. Auditor issues the integrated audit opinion (10-K)
    - Opinion on the financial statements.
    - Separate opinion on the effectiveness of ICFR (404(b)):
    - Unqualified (effective)
    - Adverse (one or more material weaknesses)
    - Disclaimer (scope limitation—very rare)
15. File Form 10-K with SEC

- Includes management report, auditor's attestation report, and disclosure of any material weaknesses.

Typical Timeline (for Dec 31 year-end companies)

- Q1–Q2: Update documentation, management testing
- Q3: External auditor interim testing (design + some operating)
- Q4: Year-end substantive testing + final ICFR testing
- Jan–Feb: Roll-forward testing, deficiency evaluation, remediation (if needed)
- Late Feb/Mar: Sign opinions, file 10-K (accelerated/large accelerated filers have tighter deadlines)

Key Frameworks Usually Used

- COSO 2013 Internal Control — Integrated Framework (most common)
- COBIT or ITGI for ITGCs

Key PCAOB Standards

- AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements
- AS 2110: Identifying and Assessing Risks of Material Misstatement
- AS 2305: Substantive Analytical Procedures (for reliance on controls)

By following the top-down, risk-based approach mandated by AS 2201, companies and auditors can efficiently complete the SOX 404 attestation while focusing effort on the areas of highest risk.

