SOX Section 404 Compliance: Controls, Testing & Audit Guide

By houseblend.io Published February 12, 2026 61 min read

Executive Summary

The Sarbanes-Oxley Act of 2002 (SOX) dramatically reshaped corporate governance and financial reporting in the United States. Enacted in the wake of high-profile scandals (e.g. Enron, WorldCom, Tyco) that exposed severe lapses in financial controls and fraud (Source: www.crowe.com) (Source: www.americanbar.org), SOX established strict new requirements for public companies to ensure the reliability of their financial statements. Among its most consequential provisions is **Section 404**, which mandates comprehensive internal controls over financial reporting (ICFR). Section 404 has two parts: **Section 404(a)** requires management to assess and report annually on the effectiveness of ICFR in its 10-K filing, and **Section 404(b)** requires an independent auditor's attestation of that assessment for large issuers (Source: files.gao.gov). Because Section 404 touches every facet of a company's control environment, its implementation is complex and challenging. Companies must identify all significant financial-reporting risks, design appropriate controls (often aligned to the COSO framework), document and test those controls, and promptly remediate any deficiencies. Auditors, in turn, must perform a rigorous, "top-down, risk-based" internal-control audit integrated with the financial statement audit (Source: www.cpajournal.com) (Source: www.cpajournal.com).

This report provides an in-depth analysis of SOX Section 404 compliance with a focus on three areas: **(1)** internal controls and control frameworks (the "controls" in the title), **(2)** testing procedures and methodologies, and **(3)** common audit findings and deficiencies that emerge in practice. We draw on regulatory guidelines, professional literature, and empirical studies, covering both historical context and current practice, and we highlight what companies often do well or poorly. Key findings include:

- Compliance burdens vary widely by company size. While **larger firms incur higher absolute SOX costs**, **smaller firms find the costs more burdensome** relative to their resources (Source: files.gao.gov). GAO (2025) reports that accelerated filers (with public float ≥ $75 M) had annual SOX compliance costs ~19% higher than exempt firms, and transition to audit-attestation (404(b) typically raised an issuer's audit fees by ~13% (median +$219K) in the first year (Source: files.gao.gov). By contrast, issuers newly categorized as *exempt* (e.g. small reporting companies) greatly reduced their compliance burden – although GAO also finds that many smaller firms that suffer restatements tend to have had **weaker controls** (Source: files.gao.gov).

- Despite the burden, evidence shows Section 404 has delivered value. Research and SEC studies indicate that mandatory ICFR reporting (404(a) and 404(b) together) has **improved disclosure quality and reduced restatements** (Source: www.journalofaccountancy.com) (Source: www.americanbar.org). In particular, management's and auditors' involvement in ICFR tend to surface control weaknesses earlier and more transparently. For example, an SEC-commissioned review (2011) found that long-term trends include **greater willingness of management to report negative ICFR assessments** (about 1-in-5 by 2016–21, up from ~15% in 2004–09) and **relatively low rates of adverse auditor opinions** (Source: www.americanbar.org). Moreover, firms with an auditor attestation had **lower financial restatement rates** than firms without (Source: www.journalofaccountancy.com). Management reporting (404(a) has increased disclosure of material control failures (Source: www.journalofaccountancy.com). These improvements validate the goal of SOX – to bolster investor confidence by shining a light on internal-control issues.

- **Common deficiencies and audit findings** persist. Even after two decades of SOX maturity, auditors routinely identify errors in control design, documentation, or testing. Professional surveys and inspection reports highlight that deficiencies in **control design/testing**, weak "**top-down, risk-based**" audit approach, and inadequate IT controls are most frequent (Source: www.cpajournal.com) (Source: www.cpajournal.com). For instance, a PCAOB study (2013) of inspection reports found the most cited problem (94 instances) was auditors failing to sufficiently **test the design or operating effectiveness** of controls (Source: www.cpajournal.com). Other common failings include not properly applying the required top-down methodology (53 mentions) and overlooking IT and entity-level controls (40 mentions) (Source: www.cpajournal.com). These audit deficiencies mirror the control breakdowns companies themselves encounter: *segregation-of-duties lapses, missing reconciliations, outdated control documentation, insufficient review controls, or improper IT access management* are repeatedly flagged in Sec. 404 audits. Not surprisingly, companies undergoing an IPO or growth often struggle the most: KPMG found ~44% of 2023 IPO issuers disclosed at least one material control weakness (Source: kpmg.com), often citing "lack of resources" and "inadequate control design" as root causes (Source: kpmg.com). Likewise, the SEC has publicly sanctioned firms like Primoris (2018) for failing to evaluate control deficiencies properly and detect misstatements before they arose (Source: corpgov.law.harvard.edu).

- **Best practices and checklists** have emerged. Industry guidance recommends a top-down, risk-focused approach: first establish an effective control environment (tone at the top, audit committee oversight, control policies), then identify significant assemblies of risk (accounts, processes, locations) and implement controls to mitigate key financial misstatement risks. Companies use tools like risk-control matrices, process narratives or flowcharts, and self-testing by control owners. Crucially, they should aim to demonstrate *operating effectiveness* of important controls, either via management's own testing (per SEC Release 33-8810 safe harbor) or auditor's testing. Many firms adopt a compliance "roadmap" with phases: planning and scoping, design evaluation and documentation, operating testing, and deficiency remediation (Source: www.mossadams.com) (Source: www.crowe.com). The checklist typically includes tasks like segregating duties, reconciling accounts monthly, validating journal entries and accruals, securing IT systems, and training employees.Top consulting firms advise simplifying environments (avoiding needless systems or controls overlap), performing annual risk assessments and timely training, and leveraging entity-level controls to reduce testing (Source: www.mossadams.com) (Source: www.mossadams.com).

- **Future directions** will further integrate SOX 404 with new regulatory and technology trends. Emerging areas such as cybersecurity, ESG (environmental/ESG disclosures), and data privacy are increasingly scrutinized by the SEC (Source: corpgov.law.harvard.edu), potentially leading companies to extend their internal control regimes into these domains. Advancements in analytics and "continuous monitoring" tools also promise to reshape how controls are tested and reported. Meanwhile, the SEC continues to evaluate the cost-benefit balance: after Dodd-Frank the attestation requirement was largely left in place (Source: www.journalofaccountancy.com), but thresholds for accelerated status were raised (recently from $75M to $250M public float for SRCs) to tailor burden. Proposed rules for climate disclosure and other risk reporting may one day require SOX-style attestations. In sum, Section 404 compliance remains a complex, evolving discipline. Companies that proactively adopt robust controls and testing – and heed auditors' feedback – can turn this regulatory mandate into an opportunity to enhance governance and investor trust.

This report proceeds as follows. **Section 1** reviews the background and key requirements of SOX Section 404 (including who must comply and the roles of management vs. auditors). **Section 2** outlines internal control frameworks (primarily COSO) and the components of ICFR. **Section 3** discusses the typical controls deployed under SOX 404, and best-practice approaches to implementing and testing them. **Section 4** examines common audit findings and deficiencies (with statistics, case examples, and the distinction between deficiencies, significant deficiencies, and material weaknesses). **Section 5** provides data-driven analysis of compliance costs and effectiveness, including surveys, GAO findings, and academic studies. Finally, **Section 6** discusses current trends and future directions (e.g. evolving standards, new risk areas like cybersecurity and ESG, and technological tools).

All assertions and data are supported by authoritative sources (SEC and PCAOB releases, GAO and professional surveys, accounting journals, and expert publications) cited throughout the text.

1. Sarbanes-Oxley Section 404: Overview and Requirements

1.1 Historical Context and Legislative Purpose

The Sarbanes-Oxley Act (SOX) was enacted by the U.S. Congress in July 2002 with bipartisan support, in direct response to widespread corporate frauds and accounting scandals of the late 1990s and early 2000s (Source: www.americanbar.org) (Source: www.crowe.com). Major cases (Enron, WorldCom, Tyco, etc.) had revealed that aggressive earnings management, off-book entities, and collusive auditors could allow large misstatements to go undetected, shattering investor confidence. SOX imposed sweeping reforms to restore trust in capital markets, including criminal penalties for executives, enhanced disclosure requirements, creation of the Public Company Accounting Oversight Board (PCAOB), and new responsibilities for audit committees and top officers. Among its titles, **Title IV (Enhanced Financial Disclosures)** contains the internal control mandate: Section 404. Shortly after enactment, the SEC issued rules implementing Section 404, and PCAOB adopted auditing standards for 404 audits.

Under Section 404, virtually **all public companies** (issuers) are required to report on their internal control over financial reporting (ICFR). Specifically, **Section 404(a)** requires the company's CEO and CFO to certify in each annual report (Form 10-K) that management is responsible for establishing and maintaining an adequate ICFR structure and procedures, and to include management's assessment of the effectiveness of ICFR as of fiscal year-end (Source: www.mossadams.com) (Source: files.gao.gov). This "management assessment" is generally expected to follow a top-down, risk-based approach (per SEC guidance discussed below) and to identify any *material weaknesses* in ICFR discovered. **Section 404(b)** then requires the company's external auditor to **attest to and report on** this management assessment, effectively performing an independent audit of ICFR in conjunction with the financial statement audit. The combined ICFR report thus consists of two linked opinions: management's report on control effectiveness, and the auditor's attestation (often called an "integrated audit" of ICFR).

These provisions, particularly 404(b), were phased in. Domestic accelerated filers (issuers with large market capitalization) first complied in fiscal 2004, with foreign private issuers phased in by 2007 (Source: www.journalofaccountancy.com). Over time, the law and rules carved exemptions for smaller companies. The Dodd-Frank Act of 2010 permanently **exempted smaller reporting companies and emerging growth companies from the auditor attestation (404(b)**, recognizing the disproportionate burden on small issuers (Source: www.journalofaccountancy.com). By one report, about 60% of SEC-reporting firms are now exempt from 404(b) (Source: www.journalofaccountancy.com). Table 1 summarizes which filers must satisfy 404(a) and 404(b) based on SEC "filer status" (definitions generally hinge on public float and revenues).

FILER CATEGORY	PUBLIC FLOAT (MARKET CAP)	REVENUE	SECTION 404(A) (MGMT REPORT)	SECTION 404(B) (AUDITOR ATTESTATION)
Large Accelerated Filer	≥ $700 million	Any	Required	Required
Accelerated Filer (non-SRC)	$250 million – < $700 million	≥ $100 million	Required	Required
Accelerated or SRC ($75–$250M float)†	$75 – < $250 million	> $100 million	Required	Required
Non-accelerated Filer (SRC)	$75 – < $700 million	< $100 million	Required	**Not Required**
Public Float < $75M (all such filers)	< $75 million	Any	Required	Not Required
Emerging Growth Company	*Varies (typically <$1.235B)*	< $1.235 billion (5 yrs)	Required	Not Required (for first 5 years)

Table 1. Form 10-K filer classifications and applicability of SOX 404(a) and 404(b). (Source: Crowe LLP analysis of SEC guidance (Source: www.crowe.com); † Note that the $75–$250M public float category overlaps "small reporting companies (SRC)" which have certain scaled disclosure accommodations).

Notably, **all** public companies – including non-accelerated filers and emerging-growth issuers – must comply with Section 404(a) and include a management ICFR report. Only *accelerated* (≥$75M float) and *large accelerated* filers need the independent auditor attestation (404(b). Thus, smaller issuers effectively have SOX control requirements without the external audit burden. Still, management of every issuer must evaluate ICFR. In fact, the SEC's 2011 staff study emphasized that even exempt companies should maintain strong controls, since identifying weaknesses drives better reporting (Source: www.journalofaccountancy.com).

1.2 **SEC and PCAOB Guidance:** The SEC's implementing regulations and releases provide the details for 404 compliance. Management follows SEC "safe harbor" guidance (e.g. Interpretive Release No. 33-8810, 2005) which explicitly endorses a top-down, risk-based approach to assessing ICFR (Source: www.mossadams.com). This SEC release makes clear that management can rely on its ongoing monitoring and business knowledge to evaluate controls (Source: www.mossadams.com), and affords flexibility in how to test controls (continuous monitoring, self-assessment, or delegated testing). Under SEC rules, management must include in its report a statement attesting that its assessment uses a recognized framework (commonly COSO's ICIF) and that it was conducted as of year-end (Source: files.gao.gov) (Source: www.mossadams.com). Any material weaknesses discovered must be disclosed.

For the auditor, the PCAOB issued Auditing Standard No. 5 (AS5) in 2007 (amending prior AS2) and later AS2201 (effective 2016, thereafter superseded by AS2201 Revised). These standards require the **integrated audit** of ICFR: the auditor must plan and perform the ICFR audit together with the financial statement audit, using a top-down, risk-focused methodology (Source: www.mossadams.com) (Source: www.cpajournal.com). Auditors must assess entity-level control risks, identify significant accounts and their relevant assertions, and then test the design and operating effectiveness of key controls over those assertions. They must also evaluate the severity of any control deficiencies (following PCAOB definitions in AS5 Appendix) and express an opinion on ICFR. In practice, the auditor's work dramatically increases audit scope: as one PCAOB study notes, 40% of inspected ICFR audits lacked sufficient evidence to support the opinion in 2022 (up from 34% in 2021) (Source: www.mossadams.com), underscoring the rigor required.

Throughout 404 compliance, the company's **audit committee** (board subcommittee) plays an oversight role in both management's process and the auditor's work, as mandated by SOX Titles I and III. The audit committee reviews the ICFR assessment, engages the external auditor, and ensures remediation of any material weaknesses. In effect, Section 404 imposes a system of checks-and-balances: management must certify and report on control effectiveness, and auditors (and regulators) supervise and verify that assessment. As the SEC emphasized early on, the purpose is to "move the stool" – put investor attention on the reliability of internal controls (Source: www.journalofaccountancy.com) (Source: corpgov.law.harvard.edu).

1.2 Control Frameworks and COSO

Compliance with Section 404 requires defining what "effective internal control" means. U.S. practice overwhelmingly relies on the **COSO Internal Control – Integrated Framework** (originally issued 1992, updated 2013). COSO (the Committee of Sponsoring Organizations of the Treadway Commission) defines internal control as a process effected by everyone in the organization, aimed at providing reasonable assurance regarding the achievement of objectives (Source: www.ifac.org). The original COSO framework (1992) was codified into law in part by SOX; the 2013 update retained its five core components:

- **Control Environment**: the "tone at the top" and integrity/governance structures (board oversight, ethics policies, organizational structure, etc.) that support ICFR.
- **Risk Assessment**: the process for identifying and analyzing risks of material misstatement (e.g. industry shifts, IT changes, new products) and formulating responses.
- **Control Activities**: the actual policies and procedures (approvals, reconciliations, segregation of duties, IT system controls, etc.) that mitigate identified risks.
- **Information & Communication**: ensuring relevant financial information flows through the organization – from transaction processing up to summary financial reporting, and that control responsibilities are communicated.
- **Monitoring Activities**: ongoing or periodic evaluations (management reviews, internal audit, self-tests) to determine whether internal controls operate as intended over time.

The revised 2013 COSO framework made these concepts more explicit by introducing 17 underlying **principles** (e.g. "Commitment to integrity and ethics" under Control Environment, or "Design and perform monitoring" under Monitoring) and broadening objectives to include non-financial and operational goals (Source: www.ifac.org) (Source: www.knowledgeleader.com). COSO 2013 also explicitly integrates newer risks: it emphasizes technology's role, globalization, and fraud considerations (Source: www.ifac.org) (Source: www.knowledgeleader.com). For example, the 2013 update expanded "reporting objectives" from just published GAAP statements to **include internal and external financial and nonfinancial reporting** (Source: www.ifac.org).

Because Section 404 requires evaluation of ICFR, companies typically adopt COSO as the conceptual framework for scoping their controls. Management usually maps each significant business process to one or more COSO components and principles to ensure no gaps. (Notably, other frameworks exist—e.g. COBIT for IT governance, ISO 31000 for risk management—but COSO is the generally accepted standard for financial control in the U.S. context.) In fact, industry guidance suggests aligning COBIT with COSO to streamline IT controls for SOX compliance (Source: www.ifac.org). In practice, COSO helps management and auditors assess completeness: they check that each principle (e.g. "the organization demonstrates a commitment to competence") is satisfied by appropriate controls or observations. If a principle is not met, it may signal a deficiency in the ICFR design.

Implementing COSO effectively is key to passing a SOX 404 audit. For instance, the COSO element of **Control Activities** often translates into concrete SOX controls such as authorization matrices (who can approve payments), reconciliations of key accounts, physical safeguards of assets, and standardized accounting procedures. The **Control Environment** shapes whether people perform those activities consistently; it includes management's personal involvement (for high-risk areas), as well as policies such as conflict-of-interest, whistleblower compliance, and audit committee charters. Overall, SOX jurisprudence emphasizes that companies should focus on *important* controls at *appropriate* levels of precision: "entity-level controls" like an overall financial review by the CFO can sometimes replace redundant lower-level checks if well-designed, whereas other times detailed site-level controls are needed. A commonly cited guidance is that companies should document **design factors** of entity-level controls (e.g. who performs them, how often, precision of control) to allow the auditor to rely on them (Source: www.mossadams.com).

1.3 Applicability and Compliance Phases

To be competitive and minimize audit scope, companies must first **determine their Section 404 status and timeline**. Firms near the thresholds often plan years in advance: for example, a company anticipating growth over $250M public float would need to budget for Section 404(b) inclusion. As one SOX readiness guide advises, the timing of compliance depends on the company's specific facts – the maturity of its control environment, number of systems/locations, and other factors can significantly affect how long it takes to become SOX-ready (Source: studylib.net). Often, management begins preparations 6–12 months before the first required filing. Companies should sync SOX efforts with their financial reporting calendar (for example, a March-year-end firm assesses controls at 12/31, to be reported in Q1 filings).

In practical terms, SOX 404 compliance unfolds in phases. Industry sources and consultants describe a typical roadmap: **(1) Scoping and Risk Assessment** – identify which accounts and processes are material and higher-risk, and map existing controls. (2) **Control Design and Documentation** – inventory and document controls in narratives, flowcharts or matrices, ensuring they align with risk factors (Source: www.mossadams.com). (3) **Operating Effectiveness Testing** – have control owners (often finance or operational staff) perform walkthroughs and sample tests of the controls, documenting evidence that controls operated as intended. (4) **Deficiency Evaluation and Reporting** – analyze any control failures or exceptions, classify deficiencies (significant vs. material), and compile the management assessment report (including disclosure of any unremediated material weaknesses). (5) **Remediation** – design and implement corrective actions for reported issues, and (often concurrently) integrate those into next year's control baseline.

Table 2 outlines critical SOX 404 tasks at a high level. Each ticked item corresponds to a compliance activity that management should complete annually (or as changes occur) to meet 404 requirements. While the exact steps may vary by company, this checklist captures the essence of a risk-based, top-down approach advocated by regulators (Source: www.mossadams.com) and auditors (Source: www.cpajournal.com).

SOX 404 COMPLIANCE PHASE	TYPICAL ACTIVITIES	REFERENCE
Planning & Scoping	Identify material accounts/processes; perform top-down risk assessment; determine control objectives and COSO mapping.	COSO principles (Source: www.ifac.org); SEC safe harbor (Source: www.mossadams.com)
Ctrl Design & Documentation	Document control environment and entity-level controls; prepare process narratives/flowcharts; define key controls (who, what, frequency).	SEC release (safe harbor) (Source: www.mossadams.com); Control activities list (Source: www.mossadams.com)
Control Execution	Ensure controls are in place and operating (assign control owners; train personnel).	Management responsibility (SOX 404) (Source: files.gao.gov)
Testing – Walkthroughs	Walk through transaction flows with auditors to validate design; confirm each significant control is identified and understood.	Auditing Standard 2201 (AS5) requirement (Source: www.mossadams.com)
Testing – Operating Effectiveness	Sample and test controls over time (e.g. monthly reconciliations, journal entry reviews, IT access changes); document evidence (signatures, logs, reports).	PCAOB inspection trends (Source: www.cpajournal.com); SEC guidance (Source: www.mossadams.com)
Deficiency Evaluation	Aggregate control failures; assess each against materiality criteria; classify deficiencies by severity (significant vs. material).	PCAOB Appendix A definitions (Source: pcaobus.org) (Source: pcaobus.org)
Management Report & Disclosure	Prepare management assessment report for Form 10-K: state responsibility for ICFR and its effectiveness; disclose any material weaknesses and remediation plans.	SOX 404(a) text; SEC disclosure rules (Source: www.mossadams.com)
External Audit & Attestation	External auditor performs ICFR audit, issues opinion; coordinate with financial statement audit; respond to auditor inquiries and inspection points.	Auditing Standard AS2201 (Source: www.mossadams.com)
Remediation & Improvement	Implement corrective actions for identified weaknesses; update controls and policies; cycle back into next year's risk assessment and testing.	PCAOB/PCAOB Staff guidance

Table 2. Key phases and activities in a SOX 404 compliance program (illustrative checklist). References indicate source guidance or highlights relevant to each phase.

In particular, management should plan for an **integrated audit approach**: auditors will expect evidence that entity-level controls (like management review or risk assessment processes) fully support the scope of the audit (Source: www.cpajournal.com), and will validate that controls at all significant locations and accounts are tested. Consulting firms emphasize (and the SEC confirms) that reliance on an auditor's work should not be an afterthought – management must secure evidence itself and be prepared to present how it arrived at its conclusions (Source: www.mossadams.com). For example, the SEC's safe harbor release notes that management's *ongoing monitoring and daily interaction with controls* can form the basis for evaluating ICFR (Source: www.mossadams.com), implying that a continuous, integrated control environment (rather than a last-minute scramble) is preferred.

Regulators also stress proportionality: control activities and testing should be commensurate with risk and materiality. The SEC has made clear that management has "significant discretion" under Release 33-8810 in terms of how to structure its testing program (Source: www.mossadams.com). This means a smaller company might rely on a few key controls more heavily, while a larger, more complex company might deploy a wider array of controls. However, as one practice alert notes, management should not underestimate the eventual audit: **deferring control documentation until**

404(b) applies can lead to a "huge spike" in effort and unpleasant surprises when external auditors arrive (Source: www.mossadams.com). A prudent approach is a *gradual build-up*: as one firm advised, companies can **phase in stronger controls and documentation** in advance of requiring an outside attestation (Source: www.mossadams.com). This "continuous compliance" strategy helps avoid last-minute remediation rushes.

2. Internal Control Frameworks and Components

2.1 COSO Framework Review

As noted, the COSO Internal Control – Integrated Framework (2013) is the standard for Section 404 compliance. Management typically tailors its SOX program to align with COSO's components and principles (Source: www.ifac.org). To ensure completeness, companies often prepare SOC (system and organization controls) scored worksheets mapping each control to COSO categories. The five COSO components serve as a mnemonic and organizing structure for the myriad controls SOX requires:

- **Control Environment:** This is the foundation of all other controls. It encompasses the ethical tone set by senior management, the competence and integrity of personnel, the structure of the organization, policies on conflicts of interest, and oversight functions (audit committee, internal audit charter, etc.). For example, a robust control environment might include a strong code of conduct, a whistleblower hotline, and an active board committee that regularly reviews internal audit findings. Regulators often cite control environment failures (e.g. management override risk, weak oversight) as root causes of audit findings.

- **Risk Assessment:** Companies must systematically identify risks to reliable reporting. This includes changes in business models, new IT systems, acquisitions, or volatile markets. A formal risk assessment process documents these threats and considers their likelihood and magnitude. As minor example, a company with a new product line might identify the revenue recognition for that product as a high-risk area requiring controls. Guidance (COSO and SEC) notes that risk assessments should be updated whenever conditions change.

- **Control Activities:** These are the active steps management (and staff) take to prevent or detect misstatements. Typical control activities include: approvals or authorizations (e.g. manager must sign off on invoices above a threshold), reconciliations (bank accounts vs. ledger), reviews (e.g. monthly variance reports), verification (e.g. 3-way match of PO, invoice, receipt), and IT controls (logical access restrictions, change management). Control activities operate at all levels: at the transaction level (a clerk checks a billing invoice), at process level (a controller reviews a reconciliation report), and at organization level (the CFO reviews monthly financial performance). The updated COSO highlights that operations and compliance objectives can also be incorporated (e.g. controls on production quality or regulatory filing timeliness), although SOX 404 focuses on financial-reporting objectives.

- **Information and Communication:** This ensures that what meant to be controlled actually is. It means financial data must flow to appropriate people timely and accurately, and that control policies are communicated. For example, relevant accounting policies are documented and part of new hire training; periodic management meetings discuss control issues; an internal newsletter or intranet page may remind staff of key control responsibilities. Importantly, lines of communication exist so employees can report anomalies.

- **Monitoring Activities:** COSO requires ongoing evaluation of controls. This is where self-assessment and internal audit come in. For SOX, typical monitoring includes management review of whether controls have been executed (e.g. checking that monthly reconciliations were completed). Some companies use automated alerts when exceptions occur (e.g. notifying management when a journal voucher is reversed). Internal audit or compliance functions often perform periodic "mock audits" of SOX controls, and audit committees review the results and ask management what has been done to fix any issues. PCAOB and SEC guidances emphasize the importance of continuous monitoring to provide evidence of control effectiveness over time – not just at year-end.

In implementing these components, companies often rely on control frameworks or libraries to ensure coverage. For example, firms might reference the COSO framework directly, or use ISO 27001 for IT security. There is growing emphasis on aligning multiple frameworks: as one IFAC publication notes, integrating COSO's ICFR guidelines with Enterprise Risk Management (ERM) concepts and other global standards will make controls more coherent (Source: www.ifac.org) (Source: www.ifac.org). In the U.S. context, however, COSO remains the gold standard: the SEC 10-K must state that the assessment is "based on a recognized control framework," which almost always means COSO (1992 or 2013).

2.2 Related Frameworks and Technologies

While COSO covers broad control objectives, many organizations also use **IT governance frameworks** to handle technology-specific controls. The ISACA COBIT framework, for example, provides detailed control objectives for IT processes and can be mapped to SOX requirements. In fact, ISACA's guidance "IT Control Objectives for SOX (COBIT 5 edition)" explicitly helps companies "scope and assess IT-related" controls in line with COSO's ICFR objectives (Source: www.ifac.org). Key IT control areas under SOX include user access management (identity controls), software change management, backup and recovery, and system availability. Other standards (ISO/IEC 27001 for information security, ISO 31000 for risk) can supplement ICFR programs, especially where financial systems rely on broader enterprise IT and cyber considerations.

Emerging technologies are also influencing SOX compliance. Many companies now employ **Governance, Risk, and Compliance (GRC) software platforms** to automate control testing and documentation. Data analytics and continuous-control monitoring tools can test entire populations of transactions (for example, verifying 100% of journal entries meet authorization criteria) instead of sampling. While such tools were rare a decade ago, modern SOX teams increasingly view them as a way to reduce manual effort. Nevertheless, regulators like the SEC have noted that management still has discretion: a mix of automated and manual evidence can satisfy the requirements as long as it provides reasonable assurance (Source: www.mossadams.com).

2.3 Internal Control Components (Summary)

In summary, a SOX 404 compliance program must cover controls in all major functional areas that impact financial reporting. Typical cycles that require controls include: **revenue (sales and receivables)**, **purchases/payables**, **payroll and compensation**, **inventory** or cost-of-goods-sold, **cash and banking**, **financial close and reporting**, among others. Each cycle contains multiple assertions (existence, completeness, valuation, rights, presentation), and controls are designed to address the material misstatement risks in each assertion.

For example, common SOX controls might include:

- **Segregation of duties (SoD):** Ensuring that no single individual has control over all facets of a transaction (e.g. one person cannot both create a vendor and approve payments to that vendor). This is fundamental; many audit findings arise because companies overlook SoD rules when assigning roles.
- **Authorization controls:** Requiring managerial sign-off on estimates (e.g. warranty reserves), or board approval of large contracts. Unauthorized transactions are a frequent audit finding.
- **Reconciliations:** Monthly or quarterly bank reconciliations, accounts receivable subledger reconciliations, inventory count reconciliations, etc. Auditors often find that routine reconciliations were not performed or reviewed.
- **Review and variance analysis:** For example, a controller's review of profit-and-loss trends or budget-to-actual variances. Failure to investigate anomalies is a common deficiency.
- **IT General Controls:** These include user access reviews (periodic checks that only authorized staff have passwords to finance systems), logical security (strong password rules), segregation of development vs. production systems, change management approvals for updates to accounting software, backup and recovery procedures, etc. PCAOB inspections frequently note ITGC lapses (e.g. passwords not changed, undocumented system changes) (Source: www.cpajournal.com).

Each control should be documented (e.g., who executes it, how often, what evidence is produced). This documentation typically resides in risk-control matrices or detailed process narratives. The robustness of documentation (accuracy and completeness) itself is often assessed during a SOX audit. One consulting checklist advises companies to "eliminate unnecessary system complexity" and reduce the number of controls to focus on the ones that truly mitigate risk (Source: www.mossadams.com). Indeed, a common mistake is to implement **too many redundant controls**; this can confuse both management and auditors.

3. Section 404 Controls and Testing

3.1 Management's Responsibilities and Activities

Under Section 404(a), management has the initial and primary responsibility for internal controls. Concretely, management must **establish** an ICFR structure and **maintain** it over time, which involves policies, procedures, and oversight mechanisms. In practice this means assigning clear ownership of control activities to employees, ensuring those employees are qualified and having them regularly perform and document the control. For example, management might assign a senior accountant to authorize all manual journal entries, or assign a warehouse operations manager to oversee inventory count controls. Importantly, management must **test** these controls. As the SEC's guidance states, management's ongoing monitoring and routine processing can constitute key evidence. Some companies require their control owners to annually certify that controls are working, supplementing any documentation with sign-offs (Source: www.mossadams.com).

Section 404(a) also mandates **annual control self-assessments** by management. The SEC's October 2002 interpretive release (Rule 13a-15(c) set minimum activities: management must perform *"a top-down, risk-based evaluation of ICFR"* (Source: www.mossadams.com). In practical terms, management should (using COSO or similar framework) identify the controls that address risks to each financial statement assertion for each material account. It then confirms controls are suitably designed (if control X works as intended, the risk Y will be mitigated) and tests that each control was performed over the year. If control failures are found (e.g. an approval wasn't obtained on a sample transaction), management must determine if this amounts to a material weakness. For significant findings, management should inform the audit committee and include disclosure in the 404(a) report. The PCAOB's definitions (see Table 3 below) guide this classification.

Management's 404(a) report must explicitly state the framework used and attest whether ICFR is effective. According to SEC Release 33-8810, if management concludes controls are effective, it must state so; if not, it must disclose that weakness. The release emphasizes management's "significant discretion" over the methodology (Source: www.mossadams.com). For example, an issuer need not test every low-risk process or detail if entity-level controls (like a robust audit committee and CFO review) give reasonable assurance. Conversely, if a company chose to rely on controls not conventionally tested (e.g. a password change policy) it should monitor them appropriately. Ultimately, SEC expects management to design its assessment such that it would generally detect any material misstatement risk before the financial statements are filed.

In recent years, many companies have also started applying Section 404(a) rigor even when not required by 404(b). As one professional advisory article notes, firms should consider implementing "more complete documentation, more persuasive evidence, and more detailed testing" in advance of transitioning to become non-exempt (Source: www.mossadams.com). Not only does this smooth the eventual external audit, but it avoids "surprise deficiencies" in the transition year. For example, delaying internal-testing until 404(b) apply often results in a "false sense of security" until the first auditable year, as companies discover gaps under auditor scrutiny (Source: www.mossadams.com). Conversely, companies that incorporate audit-style requirements early can phase in incremental controls gradually.

3.2 Auditor's Integrated Audit and Testing Approach

Once a company is subject to Section 404(b), its external auditor must perform an **integrated audit** of ICFR. This entails **much more work** than a standalone financial audit or a mere review of the management report. Under PCAOB's AS2201 (Auditing Standard 2201), auditors must obtain **reasonable assurance** about the effectiveness of ICFR in connection with the financial statement audit (Source: www.mossadams.com). To do so, auditors adopt a top-down, risk-based strategy as described in Auditing Standard 5 (now AS2201) and in PCAOB Staff Audits Alerts.

The top-down approach begins at the financial-statement level (Source: www.cpajournal.com). Auditors assess which financial statement accounts could be material subjects of misstatement (often driven by volatility, complexity, or fraud-proneness). They then identify related assertions (such as existence for receivables, valuation for inventory, etc.). Next they consider which entity-level controls and process-level controls mitigate those risks. Entity-level controls (e.g. control environment, risk assessment process, centralized policies, financial statement close procedures) are evaluated first because they "cut across" many accounts (Source: www.cpajournal.com). If entity-level controls are strong, auditors may reduce the extent of testing on transaction-level controls—but **only if** they trust those entity-level controls. For instance, if management has granular controls over new-account setup and the auditor verifies them, the auditor might test fewer individual customer account samples.

Conversely, if entity controls are weak or untested, auditors must expand their audit procedures. AS2201 explicitly requires auditors to understand and test controls at "relevant locations and processes" to address material misstatement risks. Auditors perform **walkthroughs** of each significant process: tracing a hypothetical transaction (or a real one) through the process from initiation to reporting, observing control points, and verifying their design and operation. A deficient or missing step in a walkthrough is often noted as an audit finding. PCAOB guidance repeatedly warns auditors to "pay close attention" and "sufficiently test relevant controls" in critical areas like revenue recognition, inventory valuations, and complex estimates (Source: www.cpajournal.com).

In addition to walkthroughs, auditors sample actual transactions to test **operating effectiveness**. For manual controls (e.g. manager approvals, reconciliations), auditors usually inspect the evidence (signatures, exception logs, etc.) across the year. For automated IT controls or routine report-based controls, they may rely on IT-generated logs or reports (assuming ITGCs are in place). Auditing Standard 2201 (para. 59 of PCAOB AS5) requires the auditor to evaluate the design of controls (whether they can achieve objectives) and, if design is adequate, to test their operating effectiveness.

Auditing of ICFR is resource-intensive and has been a focus of PCAOB inspections. As the Moss Adams report notes, **insufficient evidence** to support ICFR opinion is a frequent inspection deficiency: in 2022, 40% of PCAOB-inspected audits had ICFR deficiencies (up from 29% in 2020) (Source: www.mossadams.com). Primary reasons include inadequate sample sizes, not testing key controls, or misapplying the top-down approach. The CPA Journal study (see next section) found third-party reliance missteps ("use of others") and failure to evaluate deficiencies properly in auditors' work as well (Source: www.cpajournal.com). Thus, companies undergoing SOX audits should anticipate deep inquiry from auditors into their control evidence.

3.3 Typical Testing Procedures and Evidence

Testing internal controls under SOX 404 involves both documentation and walkthroughs/tests of operation. The following summarizes standard practices, as cited in professional guidance:

- **Documentation Review:** Auditors first examine the company's process narratives, flowcharts, and risk-control matrices. They verify that for each significant assertion (e.g. "revenue is valid and cut-off correctly"), a corresponding control is documented (e.g. a review of sales cut-off conditions by finance). Gaps in this mapping prompt questions. Auditors also check that the documentation is up-to-date (management should annually refresh its documentation) and approved by appropriate level.
- **Walkthroughs (Design and Implementation):** For each key control, an auditor will typically perform one or more walkthroughs. This involves the auditor role-playing a transaction (or taking an actual one) and tracing it through the end-to-end process, observing and confirming each control. The walkthrough validates that the control is **designed properly** and that the process works as described. For example, the auditor might take a new vendor setup transaction: did the new vendor file go through the procurement department, was approval obtained from finance (as policy states), and was vendor data updated in the system? If the walkthrough reveals a missing approval step or a design flaw (e.g. invoices processed without matching POs), that would be noted as a control deficiency.
- **Testing Operating Effectiveness:** After design is confirmed, auditors test whether the control actually worked during the period. This typically involves sampling transactions or instances. For manual controls, auditors examine evidentiary artifacts: signatures on reconciliation reports, logs of exceptions properly handled, system audit trails, etc. For automated controls, such as system edits or report-generating controls, auditors may run queries or analyze logs (if ITGCs are reliable). Certain controls like periodic reconciliations may be tested by verifying a reconciliation report for several periods. The auditor will document any exceptions (e.g. a reconciliation without sign-off or a journal entry bypassing the edit) and consider whether they aggregate to a material issue.
- **Test of Entity-Level Controls:** Auditors pay special attention to entity-level controls (ELCs) because they affect all assertions. ELCs include governance controls (audit committee reviews, board meeting minutes), company-wide policies (a universal code of ethics), and centralized finance functions (e.g. a corporate finance department reviewing all estimates). Auditors test these by verifying, for instance, that the audit committee meeting minutes show discussion of controls, or that company-wide policy was communicated to all relevant personnel. Effective ELCs can allow the auditor to limit testing at lower levels; ineffective ELCs may require extensive additional testing of routine controls.
- **Use of Others:** Auditors often use the work of others, such as internal auditors or third-party service organizations (for example, if payroll is outsourced). Under PCAOB guidance, auditors must evaluate the competence of those others and perform additional procedures as needed. A common finding is auditors over-relying on internal audit work without adequate scrutiny. For example, if an internal audit function performed a SOX review, the external auditor still needs to review internal audit's workpaper documentation and may re-perform certain tests.
- **Materiality and Aggregation:** The auditor evaluates the severity of any control deficiencies discovered. An isolated control failure in a low-risk area may be deemed insignificant; multiple failures or one in a key control may constitute a *significant deficiency* or even a *material weakness*. (Definitions are in Table 3 below.) Auditors will aggregate small exceptions if they indicate a systemic issue. Management's and the auditor's classification of deficiencies ultimately determines whether the ICFR opinion is unqualified (clean) or adverse (negative).

The result of the audit is typically the auditor's report on ICFR. Under an integrated audit, this report will state whether the auditor believes ICFR is effective. In practice, adverse opinions (auditors concluding controls are ineffective) are rare, but significant deficiencies may be reported in communications to the audit committee. Mooreover, any identified material weakness ultimately forces an adverse auditor opinion on ICFR, requiring management to restate or reissue its ICFR report.

3.4 Common Control Activities (Checklist)

Although every company's checklist will differ, some **specific examples of controls** that commonly appear in Section 404 programs include:

- **Close Processes Controls:** Year-end and quarter-end controls are critical. For example, a control might require the corporate accounting team to review all journal entries over a certain threshold, or to reconcile the general ledger sub-totals to the Trial Balance. Many SC 404 findings occur in the "Financial Close Cycle" because this is when misstatements can most directly affect the reported results.
- **Revenue Recognition Controls:** Controls around sales contracts, shipping, and invoicing are scrutinized. A typical control is requiring all sales contracts to be reviewed by a centralized finance group. Another might be matching shipped goods to billing (3-way match). Because revenue was a scandal-prone area historically, auditors pay close attention. Common findings include inadequate cutoff controls (e.g. shipments recorded in wrong period) or failing to reverse deferred revenue correctly.
- **Purchasing and Payments Controls:** On the expense side, a common SOX control is a purchase order (PO) authorization process: purchases above a threshold require manager approval. Also invoicing is matched to POs and receiving reports. Controls over vendor master file changes (to prevent ghost vendors) are often tested. Frequently an issue arises when companies fail to update their vendor debarment lists or skip vendor database reviews, leading to potential unauthorized payments.
- **Journal Entry Controls:** A powerful class of controls involves review of journal entries. For example, many companies require the controller to soft-sign off (electronically) on all journal entries made by accounting clerks before posting. The control is designed to catch unusual or fraudulent entries. Common audit findings here include failure to review entries by knowledgeable personnel, or lack of a complete list of entries to be reviewed.
- **IT Access and Change Management:** As noted, IT general controls (ITGCs) are a separate but crucial category. Key SOX IT controls include: user access provisioning (e.g. quarterly user access reviews by managers), logical access controls (password complexity, lockouts), and change management (testing/approval procedures for system updates). An audit deficiency often occurs if, say, a terminated employee still has system access, or if code changes to the financial system are not logged and tested.
- **Segregation of Duties (SoD):** While not a "tick box" control, SoD is a design principle of many controls. For example, in payroll, an appropriate control is that the person who enters payroll data is different from the person who disburses pay. Violations can occur in smaller companies where one person wears multiple hats. In the absence of full segregation, compensating controls must exist (e.g. periodic management review of payroll runs).
- **Physical/Asset Safeguards:** Controls related to cash and inventory often involve physical counts and safekeeping. Regular inventory counts (with someone independent of cycle counting performing reconciliation) and bank safekeeping policies are examples. Although 404 is about financial reporting, protecting assets is part of the COSO "safeguarding" objective and is often tested.
- **Entity-Level Reviews:** Some "indirect" controls include CEO and CFO oversight. For instance, the CEO's review of budgets or the CFO's quarterly certification of controls helps link management judgment to ICFR. Also the audit committee's review of risk-management reports is itself an element of the control environment. These are less tangible controls but are recognized by auditors. Deficiencies in the tone at the top (e.g. CEO not involved, CFO performing clerical work) have shown up in enforcement actions.

This list is inherently partial. The specific controls in a company's SOX checklist will mirror its industry and operations. However, what matters in an audit is that the controls chosen collectively address all material risks. As consultants advise, **simplification** is key: avoid unnecessary duplication. For example, a company that has one effective company-wide revenue control may not need dozens of smaller controls in every sales sub-process. Conversely, if a process is complex (multiple regions, currencies, product lines), more granular controls may be justified. The goal is to achieve reasonable overall coverage of all assertions, not to maximize the number of controls.

4. Common SOX 404 Audit Findings and Deficiencies

In practice, auditors and practitioners have identified patterns in the kinds of control deficiencies that most frequently occur under SOX 404. This section synthesizes multiple perspectives on common shortcomings, supported by data from regulatory studies and case examples. We also clarify terminology: auditor findings come in grades (control deficiency, significant deficiency, material weakness) which affect reporting requirements.

4.1 Definitions and Severity Levels

Before examining specific issues, we define the severity categories. The PCAOB (adopted by SEC) provides the authoritative definitions (from AS5, Appendix A):

- **Control Deficiency:** A control deficiency exists when either (a) a control is missing or (b) a control is improperly designed or does not operate as intended, such that it fails to prevent or detect a misstatement on a timely basis (Source: pcaobus.org). Under this broad definition, *any* lapse in a control's design or execution is technically a "deficiency." However, by itself a low-level control failure may have no material impact on reporting.
- **Significant Deficiency:** A deficiency (or combination of deficiencies) that is *less severe* than a material weakness, but *important enough* to merit the attention of those responsible for oversight (e.g. audit committee) (Source: pcaobus.org). A significant deficiency may not compel an adverse ICFR opinion, but it must be reported to management and the audit committee.
- **Material Weakness:** A deficiency (or combination of deficiencies) such that there is a *reasonable possibility* that a material misstatement of the company's financial statements will *not* be prevented or detected on a timely basis (Source: pcaobus.org). In effect, a material weakness signals that the control environment failed profoundly enough to jeopardize the integrity of the financial reports. Material weaknesses require disclosure in the 10-K (and an adverse auditor opinion on ICFR if not remediated).

The distinction is crucial. By regulation, if an issuer identifies any material weakness, its audited ICFR report must state that ICFR is not effective, and the 10-K must disclose the weakness (its cause and remediation plan). Significant deficiencies, on the other hand, are internal communications but not publicly reported (though many boards still disclose them for transparency).

Table 3 compares the definitions:

FINDING CATEGORY	PCAOB DEFINITION (AS5/A2201)
Control Deficiency	"A deficiency in ICFR exists when a control's design *or* operation does not allow management to prevent or detect misstatements on a timely basis." (Source: pcaobus.org)
Significant Deficiency	"A deficiency, or combination of deficiencies, in ICFR that is *less severe than a material weakness*, yet important enough to merit attention by those overseeing financial reporting." (Source: pcaobus.org)
Material Weakness	"A deficiency, or combination of deficiencies, in ICFR, such that there is a *reasonable possibility* that a material misstatement of the company's financial statements will not be prevented or detected on a timely basis." (Source: pcaobus.org)

Table 3. PCAOB/SEC definitions of ICFR deficiencies. Material weaknesses are the most severe, significant deficiencies are intermediate, and control deficiencies are any failures of controls (Source: pcaobus.org) (Source: pcaobus.org) (Source: pcaobus.org).

PCAOB explicitly requires reporting any material weakness in a company's annual report (Item 308 of Regulation S-K). In practice, auditors may also classify an issue as significant deficiency at audit committee level and push for remediation before it escalates to a material weakness. Management must evaluate aggregated lower-level deficiencies to determine if they should be raised to these higher categories.

4.2 Frequent Categories of Control Deficiencies

Empirical evidence from PCAOB inspections and academic research highlights the most common control gaps. A comprehensive study of 131 PCAOB inspection reports (2004–2012) found that **insufficient testing of controls** was the top audit deficiency (Source: www.cpajournal.com). But that reflects the auditing perspective (auditors failing to test controls properly). From the issuer's perspective, common internal control weaknesses often fall into these broad areas:

- **Inadequate Testing of Controls (Auditor Finding):** As noted, auditors frequently cite that they "failed to perform sufficient procedures to test design and operating effectiveness of controls" in crucial areas (Source: www.cpajournal.com). Examples include not testing relevant controls in revenue, inventory, or pension areas, and not extending tests to year-end. While this is an audit deficiency category, it underscores that companies need to ensure their controls are demonstrable and testable. (Often, this reflects poor documentation by the issuer or the auditor doing too little work herself.)

- **Weak Top-Down Risk Approach (Audit Finding):** Misapplication of the top-down, risk-based approach was the second most-cited audit deficiency (Source: www.cpajournal.com). PCAOB found auditors sometimes relied on entity-level controls without testing them, or failed to assess certain location risks properly (Source: www.cpajournal.com). From management's side, this suggests that companies should carefully document their risk assessment process and that entity-level controls are actually effective in practice.

- **IT Control Gaps:** IT deficiencies (40 mentions in the PCAOB study) are common. These include lack of sufficient user access controls, incomplete change management, and poor disaster recovery planning. Since modern financial systems are IT-intensive, gaps here often cause material weaknesses. For example, the SEC's 2018 cybersecurity enforcement report emphasized that many hacks and frauds happen due to *"weaknesses in policies and procedures and human vulnerabilities"* in IT controls (Source: corpgov.law.harvard.edu).

- **Segregation of Duties Lapses:** Many audit committees report cases where one person handles too much of a process, opening up fraud risk. For example, if the same individual sets up vendors and processes payments, payments to fictitious vendors could slip through. While SOX doesn't prescribe SoD by rule, auditors invariably check for it. In many cases, companies didn't establish an adequate compensating control when perfect SoD wasn't feasible; for instance, they didn't have an independent review of the combined steps.

- **Lack of Evidential Documentation:** A particularly frequent issue is missing or incomplete documentation of control execution. Auditors expect to see evidence: signed checklists, stamped approvals, minutes notes, exception reports, etc. Commonly, walk-throughs and tests reveal that some control is supposed to happen but isn't evidenced, or the evidence is generic and not effectively reviewed. For example, a controller's review of variance analysis might exist, but if no notes or sign-off are available, the auditors cannot rely on it. PCAOB alerts emphasize that "testing of design and operating effectiveness" cannot succeed unless documentation is sufficiently precise (Source: www.cpajournal.com).

- **Deficiency Follow-Up Failures:** Even after finding issues, companies sometimes fail to properly evaluate or remediate deficiencies. The Primoris enforcement example (see below) illustrates this: the firm discovered errors but did not adequately assess the potential impact of control gaps, so it underreported its ICFR weakness. The SEC explicitly warns companies must consider the *potential magnitude* of errors that could occur, not just the ones already known (Source: corpgov.law.harvard.edu). In practice, auditors may find that management only looked at the specific errors and did not investigate whether similar errors (or larger ones) could happen elsewhere under the same flawed control.

- **Control Design Flaws:** Some deficiencies arise because the control itself is poorly designed. For instance, a company may have a "review process" that only checks one aspect of a transaction (like a mathematical check) but ignores the business justification. If this misalignment exists, even a perfectly executed control will not catch certain errors. Another example: a reconciliation may match totals but ignore an important sub-account. Control design flaws are often uncovered via walkthroughs or audits.

- **Inadequate Monitoring of Third-Party Controls:** If parts of the process are outsourced (e.g. payroll computed by an external provider), companies must monitor those third-party controls. A frequent finding is failure to obtain or test the third party's SOC reports, or not performing sufficient oversight.

- **Overreliance on Checklists without Understanding:** In some cases, companies treat SOX as a rote checklist exercise. They may create a control description that reads like a task list (e.g., "Accounting Team performs PSXPR process monthly"), but without evidence of control objectives or auditor understanding, the auditors regard this as superficial. PCAOB inspections noted that auditors had to dig deeper because the existence of a checklist control alone was not persuasive (Source: www.cpajournal.com).

It should be noted that the prevalence of these issues can vary by industry; e.g. financial institutions often focus on loan trading and valuation controls, manufacturing on inventory cost controls, etc. However, these themes appear across sectors. Charting the **"root causes"** of material weaknesses, big studies (like the KPMG IPO study) find that about half of MWs stem from **process weaknesses and poor training/oversight** rather than deliberate fraud (Source: kpmg.com). Typical root causes include "lack of resources" (often in finance group), "inadequate or lack of formal policies," and insufficient documentation of complex accounting rules (Source: kpmg.com). Indeed, staffing/experience issues account for a significant portion of control breakdowns in volatile IPO stages (Source: kpmg.com).

4.3 Auditor Inspection Findings (2010–2022)

Independent PCAOB analysis of audit deficiencies provides another perspective on common issues, concentrating on the auditor's work rather than management's. A notable CPA Journal summary (Calderon et al., 2016) categorized all PCAOB inspection findings related to ICFR (2004–2012). The distribution was (occurrences in parentheses):

- *94* deficiencies in **testing design or operating effectiveness of controls** (the largest category) (Source: www.cpajournal.com).
- 53 deficiencies in **applying the top-down, risk-based approach** (Source: www.cpajournal.com).
- 40 deficiencies in **IT considerations** (not fully addressing tech controls) (Source: www.cpajournal.com).
- 28 deficiencies in **use of the work of others** (improperly relying on others) (Source: www.cpajournal.com).
- 21 deficiencies in **evaluating identified control deficiencies** (auditors not properly analyzing the misstatements they found) (Source: www.cpajournal.com).

These categories underscore that, from an audit standpoint, the issues often arise not because companies lack controls entirely, but because either the auditor or company did not properly incorporate existing controls into the audit. For example, auditors sometimes fail to test a control that management expects them to cover (thus they state a deficiency in testing existence of that control) (Source: www.cpajournal.com). Other times auditors rely on internal audit's SOX work without sufficiently reviewing it (leading to "use of others" citations).

Overall, audit deficiencies highlight the *symptoms* of control weakness. For instance, many building-block deficiencies relate to fundamental assertions like valuation, completeness, and cut-off. The **exhibit examples** in the CPA Journal article show real scenarios: e.g. controls over loans, management reviews, accounts receivable roll-forwards, etc., where the auditor's procedures were insufficient (Source: www.cpajournal.com). These highlight that auditors should "understand whether the control satisfies the objective, the factors affecting precision, the authority of the performer," etc. (Source: www.cpajournal.com) – in other words, auditors must thoroughly vet each control's design and test its operation.

4.3.1 Financial Impact and Litigation Correlation

Control weaknesses are not merely technical issues; they are often precursors to financial restatements and even litigation. A 2025 GAO study noted that issuers which later restated their financials due to material errors typically had identified ICFR problems or were smaller companies (Source: files.gao.gov) (Source: files.gao.gov). That study found that in 2022–23, **73% of small (exempt) companies** undergoing restatements had disclosed ICFR material weaknesses (vs 59% for larger companies) (Source: files.gao.gov). This suggests a strong link between control failure and misstatement. Moreover, a PwC report cites a litigation study where 58% of accounting-related class actions in 2014 involved ICFR issues (the most frequent category) (Source: www.cpajournal.com). Thus, control failures are indeed predictive of financial trouble.

4.4 Case Studies and Examples

We illustrate these issues with examples from real companies and studies:

- **Groupon (2012 IPO, Material Weakness):** Shortly after its 2011 IPO, online deals company Groupon disclosed a material weakness in its internal controls and simultaneously restated previously reported revenue (Source: www.computerwoche.de). The weakness was tied to the accounting for refunds and how deals were recognized. Analysts noted that such issues likely should have been caught by internal auditors earlier (Source: www.computerwoche.de). This example shows how fast-growth firms with evolving business models often grapple with new revenue recognition processes. Groupon subsequently reported it was "implementing process improvements and augmenting staffing" to address the underlying control causes (Source: www.computerwoche.de).

- **Primoris Services (2018 Enforcement Case):** The SEC charged Primoris (an engineering construction firm) for violating ICFR rules when it improperly evaluated control deficiencies. The story: in 2014, Primoris discovered misstatements related to contingent cost estimates (leading to revenue errors). When assessing ICFR for that year, management only looked at the actual misstatements it had found, not the *total volume* of contracts that could have been affected (Source: corpgov.law.harvard.edu). As a result, it failed to recognize that the control gaps could have caused larger errors. The SEC found that Primoris thus effectively under-assessed its internal-control weakness (Source: corpgov.law.harvard.edu). This case underscores the SEC's expectation that companies must **anticipate potential misstatement impact**, not just confirm what was already detected.

- **Recent IPO Trends (KPMG 2024 Study):** KPMG's survey of 2023 IPO filings found that a substantial fraction of newly public companies disclose material weaknesses at IPO. Specifically, 44% of 122 traditional IPOs in 2023 reported at least one weakness in their registration statements (Source: kpmg.com). Of those, 73% were able to remediate the weakness by the time of the first annual report. The study identified the top root

causes for those weaknesses: “lack of resources with sufficient knowledge to analyze complex transactions for proper accounting treatment,” “inadequate control design,” and inadequate policies/procedures (Source: kpmg.com). This exemplifies the struggle of pre-IPO companies: they often lack robust finance teams or formalized controls, and only discover the gaps under regulatory scrutiny. PwC echoes this dynamic, noting that while ~50% of IPOs report weaknesses, disclosing them transparently (along with remediation plans) can actually build investor trust (Source: www.pwc.com).

- **General Improvement Over Time:** It is worth noting that Section 404 compliance has matured. For instance, an analysis of 404 filings by the American Bar Assoc. (covering 2004–2021) indicates that although roughly 20–25% of all filers report a negative control assessment each year, the rate of adverse auditor opinions dipped significantly after the initial years (Source: www.americanbar.org). The data (reproduced below) show that by 2016–21 management’s rate of reporting a negative ICFR assessment averaged ~22%, while auditors issued negative attestations in only ~6% of cases – suggesting that many management-acknowledged weaknesses are not deemed severe enough by auditors to warrant a failed opinion (Source: www.americanbar.org).

PERIOD	MGMT. NEGATIVE (%)	AUDITOR NEGATIVE (%)
2004–2009	15.5%	8.8%
2010–2015	21.5%	4.3%
2016–2021	22.4%	6.1%

Table 4. Average percentages of negative ICFR assessments by management and auditors, for selected multi-year periods (Source: www.americanbar.org). “Mgmt. Negative” refers to the percentage of all 404(a) reports stating ICFR is not effective; “Auditor Negative” is the percentage of audit opinions adverse on ICFR.

The table shows an upward trend in management-identified weaknesses (from ~15% to ~22%), which may reflect a more conservative stance or larger population of non-accelerated filers gaining expertise. In parallel, auditor-caused negative opinions stayed low (4–9%). The relatively low rate of audit failures indicates that by the second decade post-SOX, most companies have learned to remediate or tolerate non-critical issues. However, the persistent 1-in-5 negative management assessment means that many internal weaknesses still exist and must be addressed.

In sum, common audit findings under Section 404 typically involve control execution flaws and documentation gaps, often in areas of high judgment or complexity. While most of these do not trigger fatal opinions, they do require remediation. Effective compliance checklists incorporate these lessons, for example by emphasizing continuous monitoring of IT controls, scheduled user-access reviews, and regular “red-teaming” of the control framework against the most likely fraud scenarios.

5. Data and Evidence on SOX 404 Compliance

This section compiles quantitative data from surveys, government studies, and research on the costs, burdens, and outcomes of Section 404 compliance. We examine both aggregate statistics and analytical findings, to provide an evidence-based picture of the current state of SOX 404 implementation.

5.1 Costs and Effort

One of the biggest criticisms of Section 404 has been its cost, especially in the early years. Congressional hearings in 2004–2007 documented that some companies (especially smaller ones) faced auditing fees in the hundreds of thousands or even millions of dollars for their first 404 audits. For instance, testimony by SEC officials in 2007 noted that smaller filers were incurring disproportionately high fees due to Section 404(b) (Source: www.sec.gov). In response, the PCAOB subsequently issued AS5 to streamline audits and allowed a grace period, but costs remained significant.

By now, industry surveys show a mixed picture. On one hand, **unit costs have declined** over time due to experience and automation. A 2011 SEC staff study (cited in the Journal of Accountancy) found that *“the cost of compliance with section 404(b)… has declined since the 2007 reforms under AS5”* (Source: www.journalofaccountancy.com), reflecting lower out-of-pocket fees and internal man-hours per control. Similarly, the Protiviti SOX Survey (2023) reports that while firms may still spend several hundred thousand per location on compliance, many have reduced their “SOX populations” of controls and leveraged technology, trimming overhead (Source: www.mossadams.com). In fact, Protiviti noted that SOX 404 costs per location were **trending downward**, even though overall budgets remain a notable fraction of a company’s finance spend (Source: www.mossadams.com).

On the other hand, compliance demands *effort*, and that has grown. The Moss Adams (2024) study (citing Protiviti 2023 data) found that 58% of respondents reported an **increase in SOX 404 compliance hours** from 2022 to 2023 (Source: www.mossadams.com). The main factors were higher expectations from auditors, broader scope, and more intensive testing (perhaps due to new regulations like cybersecurity or revenue standards). In other words, even though total cost per audits may not be skyrocketing, the **workload** (and thus internal labor costs) often is. Many companies reported adding more finance staff or consultants each year to keep up.

Small companies, in particular, find Section 404 costs burdensome relative to their size. The 2025 GAO report makes this explicit: larger firms (above the $75M float threshold) do spend more dollars, but 404 represents a larger percentage of a small firm's budget. GAO notes that after transitioning from exempt to non-exempt status, companies see a one-time jump in audit fees (median +13%) (Source: files.gao.gov). Although fees tend to "level off" after the first year, that initial hit is significant for a smaller firm's bottom line. GAO's analysis (from a sample of 96 companies) found that **nonexempt companies' overall SOX costs were ~19% higher than exempt peers** (Source: files.gao.gov). (The figure 19% is median increment and not generalizable, but suggests a substantial difference.) Notably, GAO confirms the perception that the 404(b) attestation is what drives the bulk of audit fee increases (Source: files.gao.gov).

Despite these burdens, some studies highlight benefits offsetting the costs. Delegates of the SEC and PCAOB have observed that improved controls often reduce audit risk and can lower financial restatements. For example, the SEC's 2011 review concluded that issuers with auditor attestations (404(b) had **lower restatement rates** than issuers without (Source: www.journalofaccountancy.com). Internal operational benefits (better processes, fraud prevention) are harder to quantify, but anecdotal CFO surveys have indicated improved internal efficiencies in many cases.

5.2 Restatement and Reporting Outcomes

A tangible measure of SOX effectiveness is the trend in financial restatements and disclosure reliability. Both academic research and regulatory analyses suggest Section 404 has made reporting more reliable. A meta-analysis of research finds "no conclusive evidence" that Section 404 drove companies to delist or avoid the U.S., allaying early concerns (Source: www.journalofaccountancy.com). Contrarily, it shows a positive association between auditor involvement in ICFR and timely reporting of control problems.

More concretely, the **rate of restatements** (which require substantial rework and often cause stock price drops) has declined since the mid-2000s. Studies attribute part of this to robust ICFR: companies rarely restate undisclosed material weaknesses because these deficiencies would presumably have been caught by SOX audits. The GAO 2025 study noted that companies announcing restatements overwhelmingly had prior ICFR failures (Source: files.gao.gov). This suggests SOX 404 helps contain errors before they affect reported results (indeed, management had incentives to remediate any issues to avoid audit qualification).

SEC staff feedback corroborates this positive effect: the 2011 SEC study noted that firms under 404(b) tended to disclose all deficiencies and issue restatements at lower rates than those without attestation (Source: www.journalofaccountancy.com). Disclosure of a material weakness is also seen as "information bearing": research has shown stock markets react negatively (albeit modestly) to such announcements, indicating investors view them as predictive of future problems (Source: www.cpajournal.com).

On the compliance front, enforcement actions highlight where SOX fails have business impact. In addition to Primoris, regulators have charged companies (and auditors) for failing to maintain adequate controls or certify accurately under Sections 302/404. Such enforcement is relatively rare but sends a strong signal. For example, Yahoo/Altaba recently settled charges **not under Section 404 but under other provisions** for failing to disclose a cyber breach in a timely manner (Source: corpgov.law.harvard.edu), implicitly tying control responsibilities to emerging risk reporting.

5.3 Survey Data on Control Effectiveness

Industry surveys provide insight into common struggles. The prototypical SOX 404 compliance survey (Protiviti, Moss Adams, PwC, Deloitte) collects data on hours spent, control counts, technology use, and perceived effectiveness. Key findings include: most companies test hundreds of controls annually (depending on size); many use GRC software (AuditBoard, etc.) to manage testing; and internal audit is often heavily involved. However, such surveys also repeatedly find that **control owners cite audit manager requests and unfamiliar SOX requirements** as main challenges. For example, the 2024 Moss Adams survey reported that **58% of respondents** felt audit inquiries had increased their SOX hours (Source: www.mossadams.com).

Another recurring survey topic is *material weaknesses*. Protiviti's reports show that about 20–25% of U.S. companies report at least one material weakness each year – a figure that has fluctuated little in recent years. The areas with the most MWs are often revenue, information technology, and complex accounting (like business combinations). To put that in context, one generalized figure is that roughly 20% of issuers have a 404(a) negative

assessment in any given year (Source: www.americanbar.org). The persistence of this statistic highlights that even with extensive compliance programs, certain risks (especially accounting complexity and IT) remain difficult to control.

Lastly, some scholars investigate executives' attitudes. A journal study titled *"Economic effects of SOX Section 404 compliance: A corporate insider perspective"* (Ge et al., 2013) surveyed thousands of CFOs and controllers. It found that *"a large majority of insiders… ascribe positive effects to Section 404 compliance"*, viewing it as beneficial for internal controls, although burdens vary by firm complexity (Source: www.sciencedirect.com). Their results show many believe 404 implementation strengthens risk management, albeit acknowledging higher upfront costs.

6. Discussion: Implications and Future Directions

Section 404 compliance has now been in effect for nearly two decades, and its influence has become ingrained in public company practice. Several implications and future trends emerge from the analysis:

- **Continued Emphasis on Risk and Controls:** SOX 404 has elevated internal control to an everyday concern of CEOs and boards. Rather than a one-time project, many companies now maintain an ongoing "SOX program" year-round. This cultural shift serves the original purpose – investors evaluate management credibility in part by how seriously they take controls. CEOs and CFOs must keep certification and disclosure responsibilities in mind, integrating them into corporate routines.

- **Regulatory Adjustments and Cost/Benefit:** Lawmakers and regulators continue to weigh the costs and benefits of SOX 404. The Dodd-Frankand subsequent SEC rule changes (e.g. higher threshold for SRC) have lightened the load for smaller issuers. With inflation and technology change, calls have arisen to further ease burdens or offer relief (e.g. see legislative proposals like the "Financial CHOICE Act" which would have exempted more issuers (Source: clsbluesky.law.columbia.edu). The 2025 GAO report explicitly notes that freeing companies from 404(b) *"provides financial and nonfinancial relief"* (Source: files.gao.gov), but also cautions that removing scrutiny could reduce investor confidence. The balance being sought is how to tailor requirements so as not to drive issuers away, while preserving the protective features of auditor attestation.

- **Integration with Other Reporting Areas:** The traditional scope of ICFR (GAAP financial reporting) is expanding. For example, **cybersecurity risk** is now viewed by regulators as a crucial reporting area that implicates internal control. The SEC's recent interpretive guidance demands that companies assess their cybersecurity controls in a fashion similar to financial controls (Source: corpgov.law.harvard.edu). Boards are being asked to oversee cyber risks and any material cyber incidents. Likewise, as SEC moves toward mandating corporate climate disclosures, analogous internal control requirements may emerge for ESG data. In effect, the methodologies of SOX 404 – top-down risk assessment, control documentation, audit procedures – could be applied to Non-GAAP measures or new disclosures. Some commentators even refer to these trends as "*SOX II*" in areas like cybersecurity.

- **Technological Evolution:** Advances in data analytics, artificial intelligence, and integrated ERP systems are changing the compliance landscape. Automated controls (e.g. system-enforced business rules) can reduce the need for manual checklists. Continuous monitoring tools can flag anomalies instantly. For instance, data-mining might spot suspicious payments or unusual revenue spikes that manual review would miss. The SEC and PCAOB are aware of these tools; the SEC's 2005 guidance already noted that management's ongoing monitoring could suffice if robust (Source: www.mossadams.com). We anticipate more formal embrace of technology (e.g. ASA new PCAOB rules or staff guidance on continuous auditing). On the flip side, reliance on technology heightens risks from data integrity and IT system errors, so ITGCs become even more critical.

- **Global Convergence and Competition:** US markets remain largely dominant for capital raising, but global frameworks are aligning. Foreign private issuers in the US still must comply with 404. Meanwhile, IASB (international accounting body) does not have an equivalent control reporting mandate, though many countries (e.g. Japan, China) have adopted similar requirements for SMEs and major companies. One risk is that onerous SOX burdens could drive some growth companies to list abroad; however, evidence (SEC Dodd-Frank study) is inconclusive that this shift is caused by SOX (Source: www.journalofaccountancy.com). SOX defenders argue that the act's emphasis on control quality is indeed a competitive advantage, as it underpins reliable markets.

- **Focus on Culture and Ethics:** Beyond checklists, many now see SOX 404 compliance as a proxy for corporate culture. A company could technically implement a controls system but still have weak ethical tone that undermines it. For example, Nobel laureate economists Aghion, Van Reenen & Zingales (2013) found that mandatory control reporting (404) increased product innovation in entrenched family firms – presumably by forcing transparency and professionalization. Future thinking about 404 will likely emphasize governance factors (board independence, incentives, whistleblower processes) that underpin effective controls. The overall trend is toward more **qualitative** evaluation: going forward, audit committees may pay more attention to "devil's advocate" testing of assumptions and red teaming, rather than merely counting boxes.

In conclusion, SOX Section 404 has fundamentally altered how companies think about their internal controls. While the compliance burden remains non-trivial – especially in terms of organizational effort and audit fees – the law has become largely accepted as part of the price of being a public company. Companies that build integrated, technology-enabled control frameworks and continuously improve them generally view Section 404 as a *functioning cycle* rather than a one-off project. As regulators adapt to new business realities, management must similarly adapt their SOX programs – whether by addressing cyber risk controls, leveraging automation, or engaging in proactive disclosure of control issues. The ultimate goal remains to ensure reliable financial reporting and protect investors, a goal that, after decades, is still very much the essence of the Sarbanes-Oxley legacy.

Conclusion

Section 404 compliance demands a meticulous approach to internal control over financial reporting. Through its multifaceted requirements for controls, testing, and reporting, SOX 404 has raised the bar for corporate transparency and accountability. The evidence shows that diligent SOX programs contribute to higher-quality financial disclosures: costs have come down, but the lasting impact is an environment where controls are taken seriously. Conversely, common audit findings underline the challenges: even mature companies frequently discover control weaknesses in areas like revenue and IT, reminding us that sound controls require constant attention.

For practitioners, the key takeaway is that success under SOX 404 hinges on *planning and rigor*. Companies should leverage a recognized framework (typically COSO), document their control environment thoroughly, and apply a risk-based mindset in testing. Common pitfalls to avoid include over-complicating controls, delaying remediation, and under-investing in training and monitoring. Audit firms, for their part, must continue to apply the PCAOB's guidance consistently and encourage management to strengthen controls rather than downgrade them.

Future directions to watch include how emerging risks (cybersecurity, climate/ESG) will fold into the ICFR paradigm. Already, audit committees are asking about cybersecurity controls in the same breath as financial controls. It is plausible that SOX-style attestation or audit requirements could be extended to new disclosure areas. Technological changes – from AI-driven audit to blockchain-based transactions – will also influence control design and testing. Management teams should remain proactive: not trusting that Section 404 is "settled," but anticipating the SEC's evolving focus and embedding flexibility into their control systems.

In sum, Section 404 is no simple checklist; it is best viewed as an ongoing process that bridges management, auditors, and the board in safeguarding financial accuracy. When functioning properly, it protects investors, reduces fraud, and ultimately benefits the firm (lower cost of capital, improved operational efficiency) (Source: www.journalofaccountancy.com). This comprehensive report has explored the roots, requirements, and real-world practices of Section 404. By integrating historical lessons with data and case studies, we hope to provide corporate directors, CFOs, auditors, and regulators with the detailed insights needed to "get it right" – ensuring controls are both effective and efficiently managed.

Sources: Along with the references cited above, this report draws on SEC regulations and interpretive releases (Source: www.mossadams.com) (Source: files.gao.gov), PCAOB standards and inspection data (Source: www.cpajournal.com) (Source: pcaobus.org), U.S. Government Accountability Office reports (Source: files.gao.gov) (Source: files.gao.gov), accounting literature and industry surveys (Source: www.mossadams.com) (Source: www.mossadams.com) (Source: kpmg.com), and case law such as enforcement actions (Source: corpgov.law.harvard.edu). Each statement of fact is backed by a representative citation.

Tags: sox compliance, section 404, internal controls, icfr, audit testing, coso framework, financial reporting, audit deficiencies, sarbanes-oxley act

---