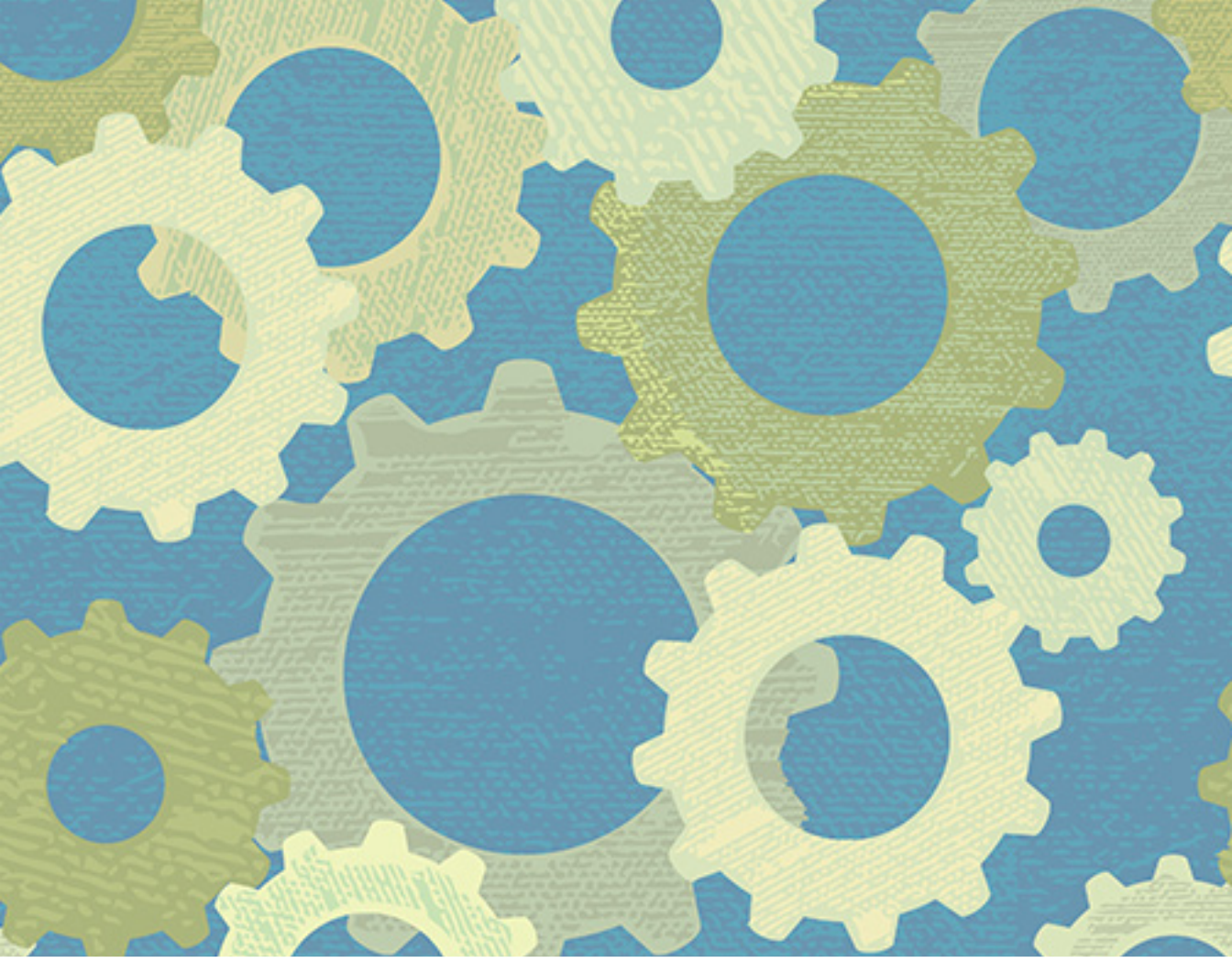
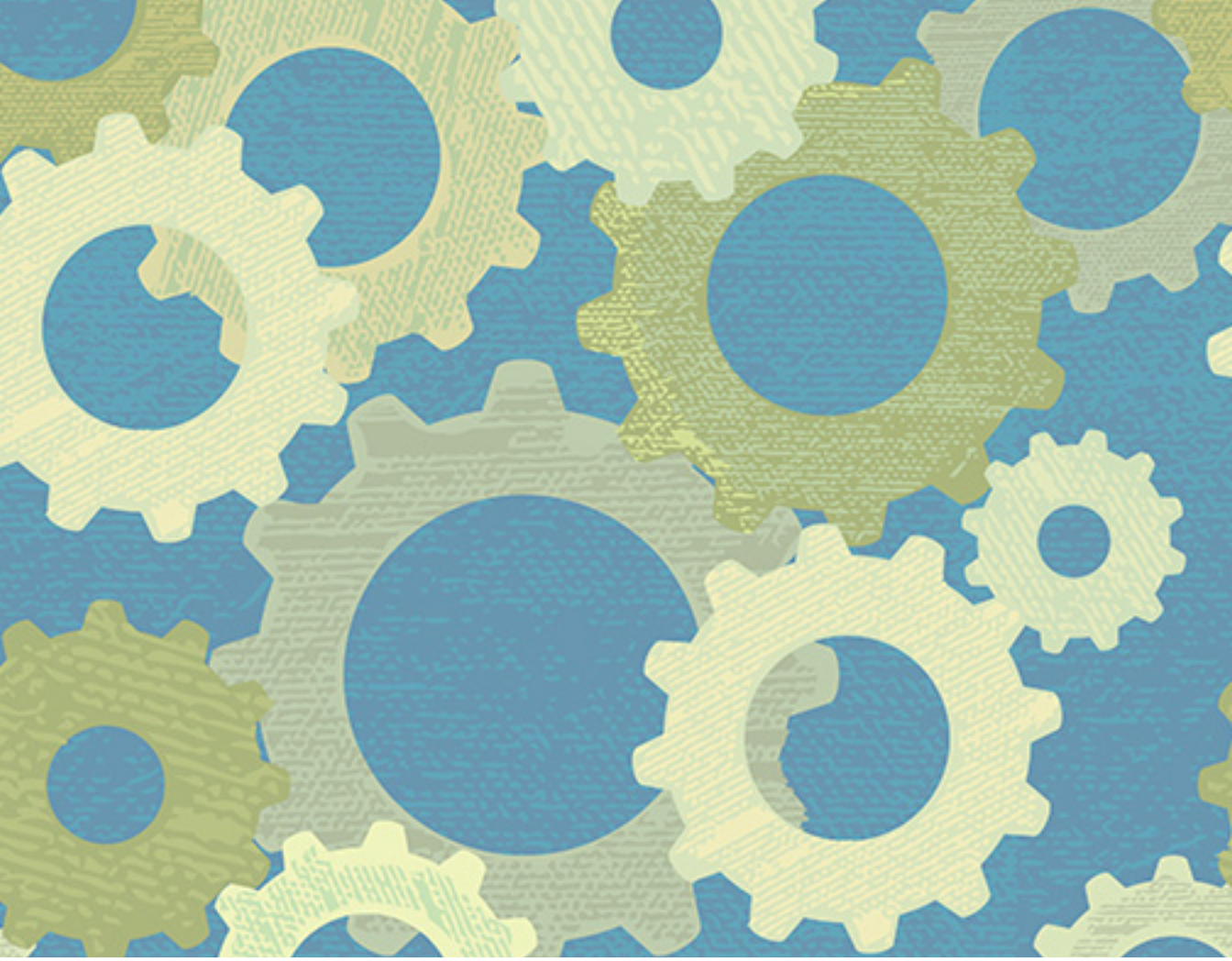


Guide to Internal Control Over Financial Reporting

CENTER FOR AUDIT QUALITY
Serving Investors, Public Company Auditors & the Markets
www.TheCAQ.org



The Center for Audit Quality prepared this Guide to provide an overview for the general public of internal control over financial reporting ("ICFR"). The Guide explains what public company ICFR is and describes management's responsibility for implementing effective ICFR. The Guide also discusses the responsibilities of the audit committee to oversee ICFR and of the independent auditor to audit the effectiveness of the company's ICFR.

A Guide to Internal Control Over Financial Reporting

Preparing reliable financial information is a key responsibility of the management of every public company. The ability to effectively manage the company's business requires access to timely and accurate information. Moreover, investors must be able to place confidence in a company's financial reports if the company wants to raise capital in the public securities markets.

Management's ability to fulfill its financial reporting responsibilities depends in part on the design and effectiveness of the processes and safeguards it has put in place over accounting and financial reporting. Without such controls, it would be extremely difficult for most business organizations — especially those with numerous locations, operations, and processes — to prepare timely and reliable financial reports for management, investors, lenders, and other users. While no practical control system can absolutely assure that financial reports will never contain material errors or misstatements, an effective system of internal control over financial reporting can substantially reduce the risk of such misstatements and inaccuracies in a company's financial statements.

Over time, effective internal control over financial reporting has become a legal obligation. Since 1977, federal law has required public companies to establish and maintain a system of internal control that provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with generally accepted accounting principles ("GAAP"). The Sarbanes-Oxley Act of 2002 added a requirement, applicable to most public companies, that management annually assess the effectiveness of the company's ICFR and report the results to the public. In addition, the Act requires most large public companies to engage their independent auditor to audit the effectiveness of the company's ICFR.

STATUTORY INTERNAL CONTROL REQUIREMENT

Congress codified the requirement that public companies have internal controls in the Foreign Corrupt Practices Act of 1977 ("FCPA"). The FCPA requires public companies to "devise and maintain" a system of internal accounting controls sufficient to provide reasonable assurance that:

- transactions are executed in accordance with management's general or specific authorization;
- transactions are recorded as necessary (1) to permit preparation of financial statements in conformity with GAAP or any other criteria applicable to such statements, and (2) to maintain accountability for assets;
- access to assets is permitted only in accordance with management's general or specific authorization; and
- the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

Source: Section 13(b)(2) of the Securities Exchange Act of 1934

What Is Internal Control?

ICFR is one element of the broader concept of internal control. Internal control includes all of the processes and procedures that management puts in place to help make sure that its assets are protected and that company activities are conducted in accordance with the organization's policies and procedures. For example, requiring that the contents of a warehouse be periodically counted and reconciled to the inventory recorded on the company's books is a control over the existence and accuracy of inventory.

In 1992, the Committee on Sponsoring Organizations of the Treadway Commission ("COSO"), an initiative of several groups with an interest in effective internal control, released a framework to assist companies in structuring and evaluating controls that address a broad range of risks. That framework defines internal control as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."

Internal Control Over Financial Reporting

ICFR — the subject of this Guide — means the controls specifically designed to address risks related to financial reporting. In simple terms, a public company's ICFR consists of the controls that are designed to provide reasonable assurance that the company's financial statements are reliable and prepared in accordance with GAAP.

Inaccuracies in a financial statement may occur, for example, due to mathematical errors, the misapplication of GAAP, or intentional misstatements (fraud). A system of ICFR should address these possibilities. The risk of fraudulent financial reporting is a key consideration in the design and operation of public company internal controls. For example, market expectations for revenues, earnings, or other targets may create pressures on management to meet these thresholds. Effective ICFR helps assure that corporate records are not purposefully misstated in response to those pressures. Controls should therefore be designed and implemented with the risk of fraud in mind and tailored to the particular circumstances of the company.

COMPONENTS OF INTERNAL CONTROL

Under the COSO framework, internal control has five components —

1. **Control Environment** — The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.

2. **Risk Assessment** — Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is the establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

3. **Control Activities** — Control activities are the policies and procedures that help ensure management directives are carried out and that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

4. **Information and Communication** — Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting.

5. **Monitoring Activities** — Internal control systems need to be monitored — a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties.

Source: COSO, Internal Control — Integrated Framework (Executive Summary)

Financial reporting often requires sophisticated decision-making and the application of informed judgment. For example, accounting areas such as estimating allowances for loan losses, valuing illiquid securities, and determining whether intangible assets are impaired require management to make judgments regarding such things as the use of assumptions and the likelihood of future events. In these kinds of reporting areas, there is typically a range of acceptable outcomes, rather than a single "correct" result.

Controls cannot remove the need for judgment or eliminate the variations in reporting inherent in situations in which a range of acceptable judgments is possible. Controls can, however, be designed and implemented to address the process by which accounting judgments are made and thereby, help provide reasonable assurance that the financial reports are presented in accordance with GAAP.

SEC DEFINITION OF ICFR

The U.S. Securities and Exchange Commission's (SEC) rules define internal control over financial reporting as "a process designed by, or under the supervision of, the [company's] principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with GAAP and includes those policies and procedures that —

1) Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;
2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and
3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements."

Source: Securities Exchange Act Rule 13a-15(f)

The Concept of Reasonable Assurance

No system of ICFR can provide absolute assurance. Internal control systems are operated by individuals, and individuals inevitably make mistakes. Further, while effective ICFR is a legal requirement for some public companies, cost considerations may affect the design of control systems. For these reasons, it is impossible to create a practical control system that will detect or prevent all potential errors. In addition, intentional misconduct, such as fraud, collusion, or management override, may prevent controls from operating as intended, regardless of how well they are designed.

Accordingly, control systems can provide reasonable, but not absolute, assurance that financial statements are reliable and prepared in accordance with GAAP. What is reasonable depends on the facts and circumstances of each particular situation. The securities laws define reasonable assurance as the degree of assurance that would satisfy prudent officials in the conduct of their own affairs.

The Control Environment

One key component of ICFR is the control environment — the structures and values within the organization. Controls designed to generate reliable financial reporting are more likely to succeed if the company's culture, including the "tone-at-the-top" established by senior management, reflects the importance of integrity and ethical values and a commitment to reliable financial reporting. Some indicators of a positive control environment include statements and actions of the board of directors and senior management that demonstrate support for effective controls; issuance and enforcement of an appropriate corporate code of conduct; and training programs that equip employees to identify and deal with ethical issues.

Control Activities

Control activities — the specific policies and procedures designed to mitigate financial reporting risk — are another key component of ICFR. Control activities are as varied as the business activities of public companies. Three concepts — segregation of duties, preventive and detective controls, and entity-level and process-level controls — are helpful to understanding control activities.

Segregation of Duties

One of the building blocks of internal control is segregation of duties. This concept involves assigning responsibility for different parts of a process to different people so that no one person can control the entire process. The importance of segregation of duties stems in part from the fact that collusion between two individuals is less likely than misconduct by a single individual. Segregation also reflects the lower probability that two persons will make the same error with respect to the accounting for a transaction. Assigning responsibility for physical access to a supply room to a different person than the individual who is responsible for maintaining the records of the supplies inventory is an example of segregation of duties.

Preventive and Detective Controls

In broad terms, controls fall into two categories — preventive controls and detective controls. **Preventive controls** are intended to prevent the occurrence of an activity that is not consistent with control objectives. For example —

- **Separating Approval and Payment.** A requirement that an employee who is authorized to initiate a payment to a vendor is not also authorized to sign vendor payment checks would be a preventive control. Among other things, such a control is designed to reduce the risk of unauthorized payments.
- **Limiting Access to IT Systems.** Controlling access to software programs related to accounting or payment functions through the use of passwords and access codes is another type of preventive control. Limiting the persons who can change IT programs reduces the risk of unauthorized transactions.

Detective controls are intended to identify errors or unauthorized activities after they have occurred so that corrections can be made in a timely manner. For example —

- **Reconciliations.** Independently comparing two sets of records that relate to the same transaction and analyzing any differences is a detective control. Reconciling the cash account balance on the company's books to its bank records could identify whether any payments recorded by the company were not received by its bank, or whether any withdrawals reported by the bank were not accounted for by the company.

- **Performance Monitoring.** Comparing operating results to budgets or forecasts, or to the results in prior periods, could be a way of highlighting unusual activities. Examining deviations might uncover errors in the records reflecting operating results or unanticipated changes in business activities.

Entity-Level and Process-Level Controls

Entity-level controls are designed to provide reasonable assurance that objectives related to the company as a whole are met. Such controls have a pervasive effect on the company's system of internal control. Audit committee oversight of financial reporting and a CFO's review of differences between the company's monthly budget and actual expenditures are examples of entity-level controls.

Other controls operate at the process, transaction, or application level. A **process-level** control pertains to a single activity. Requiring that delivery receipts be matched with vendor invoices before a vendor payment is authorized is an example of a process-level control.

Scaling ICFR to the Company

The design, implementation, and evaluation of controls need to be tailored to the size and reporting risks of the company. Designing and maintaining effective ICFR becomes more challenging as the size of a business and the scope of its activities increase. At the same time, smaller firms also may face some difficult control issues. For example, the risk of management override of controls can be greater in a smaller organization in which company officials have more direct involvement with operations and with the recording of transactions. In addition, a small company may not have sufficient personnel to fully implement segregation of duties across all processes. Nevertheless, smaller public companies still must implement a control system that will provide reasonable assurance that financial statements are prepared in accordance with GAAP and are free of material misstatements.

Management Has Responsibility for ICFR

A company's Chief Executive Officer has overall responsibility for the management of the company, including the design, implementation, and monitoring of ICFR and internal control more broadly. While management structures vary, in many companies, the Chief Financial Officer or the Chief Accounting Officer and his or her staff have day-to-day responsibility for ICFR.

As a practical matter, ICFR is implemented by individuals throughout the company, and it is important that competent, well-trained individuals are involved in the design and oversight of ICFR. Managers at all levels of the company need to be accountable for the effective operation of controls in their areas. Each business process, such as sales, purchasing, advertising, and manufacturing, should be subject to controls designed to provide reasonable assurance that the process operates effectively and that records accurately reflect individual transactions. Managers of business units also are responsible for instilling in their employees an understanding of, and respect for, the controls related to the unit's activities. A control breakdown in one process or activity could result in an undetected material misstatement, regardless of the effectiveness of the rest of the control system.

The Audit Committee of the Board of Directors Has Oversight Responsibility for ICFR

The board of directors has general oversight responsibility for all of the company's activities, including the preparation of financial statements and the design and operation of controls. The board's oversight of ICFR is delegated to the audit committee, which has specific responsibility for overseeing financial reporting under the Sarbanes Oxley Act. The audit committee's activities usually include review of the assessment of financial reporting risk; discussion with management of significant control deficiencies and their potential impact on financial reporting; and evaluation of the quality of financial reporting and related disclosures. Management officials with responsibility for ICFR are expected to keep the audit committee apprised of the operation and effectiveness of controls. If the company has an internal audit staff, its work often includes testing controls and informing the audit committee of its findings relative to ICFR.

Under the Sarbanes-Oxley Act, the audit committee also is responsible for hiring and overseeing the activities of the independent auditor. The auditor's communications with the audit committee are an important source of information related to the company's ICFR. The Public Company Accounting Oversight Board's (PCAOB) auditing standards require that the auditor communicate to the audit committee an overview of the audit strategy, which typically includes a discussion of ICFR, based on the auditor's audit planning work.

Management Reporting on the Effectiveness of ICFR

Section 404 of the Sarbanes-Oxley Act requires (with certain exceptions) all public companies to annually assess the effectiveness of ICFR and report the results. Management also has responsibility to disclose any significant changes to its ICFR system in its quarterly reports. The discipline of performing an ICFR assessment, coupled with the requirement to report the results in a public filing, affords investors increased confidence in the reliability of financial statements.

In performing its assessment, management must determine whether it has implemented controls that adequately address the risk that a material misstatement in the company's financial statements would not be prevented or detected on a timely basis and whether those controls are operating effectively. The SEC has recommended that management's assessment of ICFR take a top-down, risk-based approach. Under that approach, management first focuses on entity-level controls and then on significant accounts and significant processes and, finally, on control activities. While management's assessment must cover the company's ICFR as a whole, it should devote the greatest attention to the areas that pose the highest risk to reliable financial reporting.

ICFR Deficiencies

A deficiency in ICFR exists if the design or operation of a control does not allow management or employees, in the normal course of performing their assigned duties, to prevent or detect misstatements on a timely basis. When deficiencies in the design or operation of a control are found, management needs to assess how serious the impact may be on the integrity of the company's financial reporting processes. More serious deficiencies are classified as either significant deficiencies or as material weaknesses.

For purposes of SEC reporting, if a single **material weakness** in ICFR exists, then ICFR is not effective, regardless of the effectiveness of the rest of the controls. A material weakness means that there is a reasonable possibility that the company's controls will not prevent or detect a material misstatement of the company's financial statements on a timely basis.

It is important to understand that a material weakness in ICFR does not necessarily mean that the company's financial statements are misstated; rather, it means that there is a reasonable possibility that the company's controls would not have prevented or detected a material misstatement on a timely basis.

THE HIERARCHY OF ICFR DEFICIENCIES

A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company's financial reporting.

A deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Source: PCAOB Auditing Standard No. 5

ICFR and the Auditor

Section 404 of the Sarbanes-Oxley Act requires most large public companies to have their independent auditor report on ICFR effectiveness. Under PCAOB standards, the ICFR audit and the financial audit are integrated – that is, both audits are performed as a single, mutually reinforcing, process. Like management's assessment, the ICFR audit should follow a top-down, risk-based approach that considers the entire system of ICFR, but focuses greater attention on the controls over financial reporting areas most susceptible to material misstatement.

Because of concerns about the cost of an ICFR audit for companies with more limited resources, Congress has exempted smaller public companies, and certain newly-public companies, from the requirement that the company's auditor express an opinion on the effectiveness of ICFR. However, even in a financial statement-only audit, the auditor is still required, as part of assessing audit risk, to obtain an understanding of each component of the company's ICFR. While the auditor is not required to test internal controls in these audits, if he or she concludes that there are material weaknesses or significant deficiencies in the controls, the weaknesses or deficiencies must be reported in writing to management and the audit committee.

WHAT PUBLIC COMPANIES ARE NOT REQUIRED TO HAVE AN ICFR AUDIT?

In general, large public companies that file annual reports with the SEC are required to include in their annual report an opinion from the company's financial statement auditor on the effectiveness of the company's ICFR. Several types of companies, however, are exempt from this requirement. These exempt companies include:

- **Investment companies.** Mutual funds, and other types of investment companies, are essentially pools of securities. Such funds do not themselves engage in any business activities.
- **Non-accelerated filers.** Companies that file reports with the SEC, but have a public float (that is, securities available for public trading) of less than $75 million are referred to as non-accelerated filers because they are not subject to the same filing deadlines as larger (accelerated) filers.
- **Emerging growth companies.** During the five years following its first registered public sale of common stock, a company that has total annual revenue of less than $1 billion is an emerging growth company ("EGC"). Such a company loses its EGC status if it becomes a "large accelerated filer" (generally this requires an aggregate worldwide public float of at least $700 million) or if it issues more than $1 billion of nonconvertible debt in a three-year period.

What ICFR Means for Investors

Investor confidence and the efficient operation of our capital markets depend on reliable public company financial reporting. Reliable financial reporting depends, in turn, on an effective system of internal control over the process of preparing the financial statements. Designing and implementing controls can be a challenging process, requiring the time and attention of both senior management and the audit committee. These activities are, however, one of the bedrocks of the financial reporting system that underpins our securities markets.

SOURCES OF ADDITIONAL INFORMATION
CONCERNING INTERNAL CONTROL OVER FINANCIAL REPORTING

COSO, *Internal Control – Integrated Framework* (1992)*

COSO, *Internal Control over Financial Reporting – Guidance for Smaller Public Companies* (June 2006)

COSO, *Internal Control — Integrated Framework: Executive Summary* (Exposure draft, September 2012)

COSO, *Internal Control — Integrated Framework: Internal Control over Financial Reporting: A Compendium of Approaches and Examples* (Exposure draft, September 2012)

PCAOB Release No. 2007-005, *Auditing Standard No. 5* (Adopting release, May 24, 2007)

PCAOB Staff Views, *An Audit of Internal Control over Financial Reporting That is Integrated with an Audit of Financial Statements: Guidance for Auditors of Smaller Public Companies* (January 23, 2009)

Securities Act Release No. 8238, *Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports* (June 5, 2003)

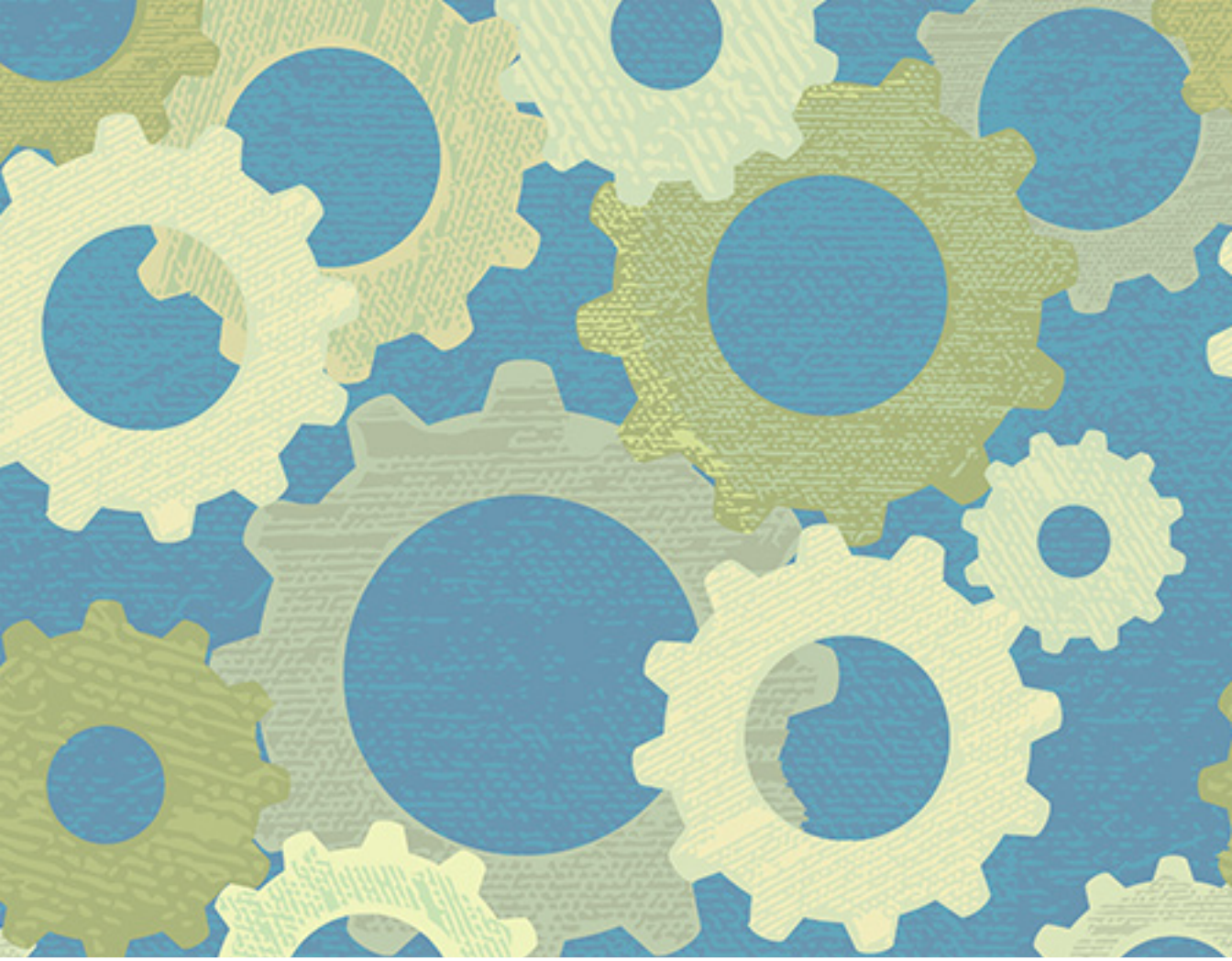
Securities Act Release No. 8809, *Amendments to Rules Regarding Management's Report on Internal Control Over Financial Reporting* (June 20, 2007)

Securities Act Release No. 8810, *Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934* (June 20, 2007)

Securities Act Release No. 8829, *Definition of the Term Significant Deficiency* (August 3, 2007)

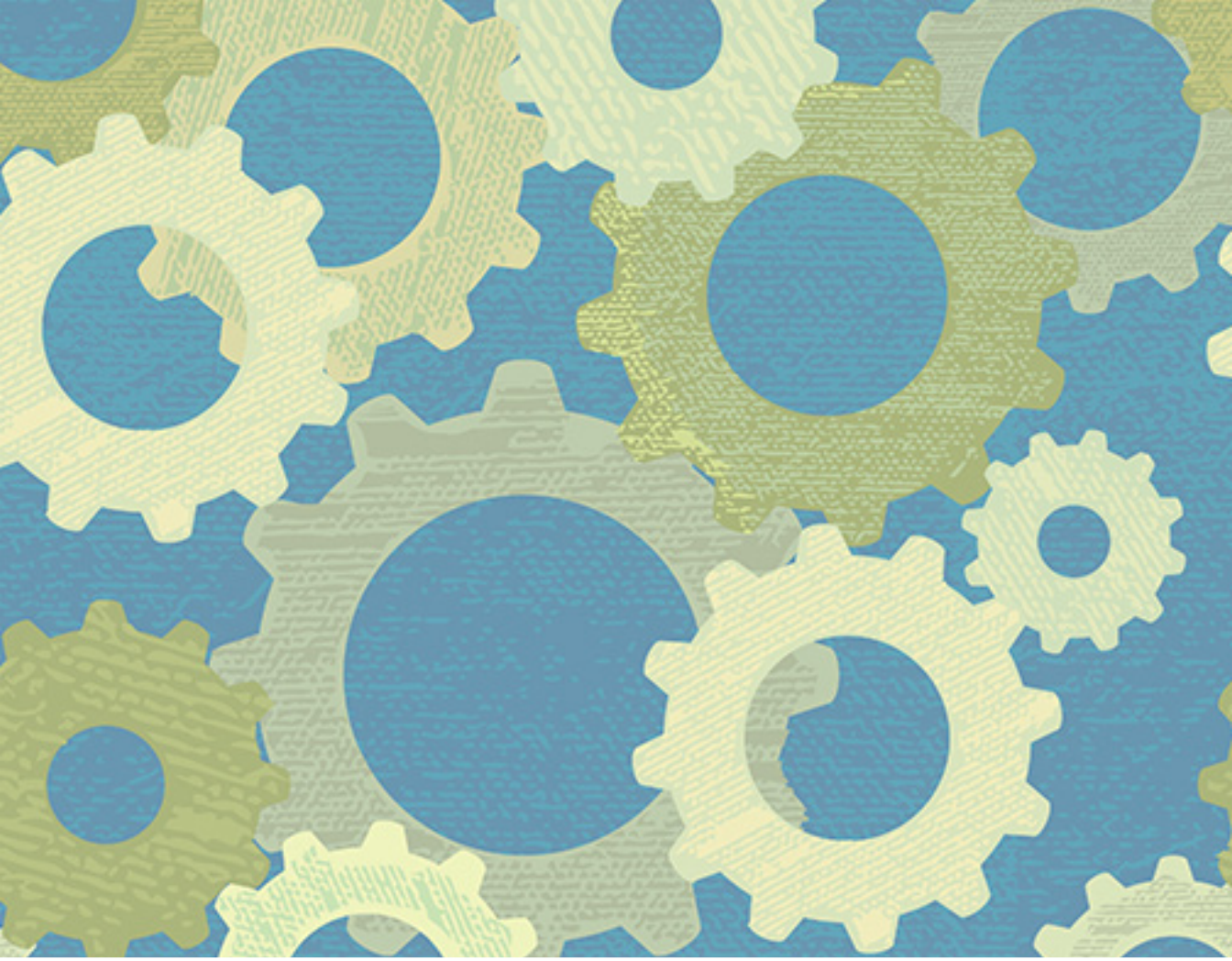
SEC Office of the Chief Accountant, Division of Corporation Finance, *Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports: Frequently Asked Questions* (September 24, 2007)

* COSO is updating its framework and has issued several exposure drafts for public comment. The final version of the updated framework is expected to be issued in 2013.



ABOUT THE CAQ

The Center for Audit Quality (CAQ) is an autonomous public policy organization dedicated to enhancing investor confidence and public trust in the global capital markets. The CAQ fosters high quality performance by public company auditors; convenes and collaborates with other stakeholders to advance the discussion of critical issues requiring action and intervention; and advocates policies and standards that promote public company auditors' objectivity, effectiveness and responsiveness to dynamic market conditions. The CAQ is based in Washington, D.C. and is affiliated with the American Institute of Certified Public Accountants.



CENTER FOR AUDIT QUALITY
Serving Investors, Public Company Auditors & the Markets
Affiliated with the American Institute of CPAs

1155 F Street, NW | Suite 450
Washington, DC 20004

202-609-8120 | TheCAQ.org