CENTER FOR AUDIT QUALITY

GUIDE TO INTERNAL CONTROL OVER FINANCIAL REPORTING

ABOUT THE CENTER FOR AUDIT QUALITY

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 that require action and intervention; and advocates policies and standards that promote public company auditors' objectivity, effectiveness, and responsiveness to dynamic market conditions. Based in Washington, DC, the CAQ is affiliated with the American Institute of CPAs.

GUIDE TO INTERNAL CONTROL OVER FINANCIAL REPORTING

CONTENTS

02 INTRODUCTION

04 KEY ICFR CONCEPTS

04 INTERNAL CONTROL

04 INTERNAL CONTROL OVER FINANCIAL REPORTING

06 REASONABLE ASSURANCE

07 THE CONTROL ENVIRONMENT

07 CONTROL ACTIVITIES

07 *SEGREGATION OF DUTIES*

08 *IT GENERAL CONTROLS*

09 *ENTITY-LEVEL AND PROCESS-LEVEL CONTROLS*

09 *PREVENTIVE AND DETECTIVE CONTROLS*

11 SCALING ICFR TO THE COMPANY

11 ICFR DEFICIENCIES

12 ICFR ROLES AND RESPONSIBILITIES

12 MANAGEMENT

13 MANAGEMENT REPORTING ON THE EFFECTIVENESS OF ICFR

13 INDEPENDENT AUDITORS

13 AUDIT COMMITTEES

15 WHAT ICFR MEANS FOR COMPANIES, INVESTORS, AND MARKETS

INTRODUCTION

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 that informs decision making. 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 operating effectiveness of the controls 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 misstatements, an effective system of internal control over financial reporting (ICFR) can substantially reduce the risk of such misstatements in a company's financial statements.

THE CENTER FOR AUDIT QUALITY HAS PREPARED THIS GUIDE TO PROVIDE THE PUBLIC WITH AN OVERVIEW OF ICFR.

Congress codified the requirement that public companies have internal accounting controls in the Foreign Corrupt Practices Act of 1977 (FCPA). This federal law requires public companies to establish and maintain a system of internal accounting controls sufficient to provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles (GAAP). The Sarbanes-Oxley Act of 2002 (SOX) 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. SOX also enhanced audit committee oversight responsibility related to ICFR and requires most large public companies to engage their independent auditor to audit the effectiveness of the company's ICFR.

The Center for Audit Quality has prepared this guide to provide the public with an overview of ICFR. The guide explains what public company ICFR is and describes management's responsibility for implementing effective ICFR. It 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.

THE STATUTORY INTERNAL ACCOUNTING CONTROL REQUIREMENT

The FCPA requires public companies to "devise and maintain" a system of internal accounting controls sufficient to provide reasonable assurance that[1]

- 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 regarding any differences.

1 Section 13(b)(2)(B) of the Securities Exchange Act of 1934.

KEY ICFR CONCEPTS

INTERNAL CONTROL

ICFR is one element of the broader concept of internal control. The latter is defined by the Committee on Sponsoring Organizations (COSO) of the Treadway Commission—an initiative of several groups with an interest in effective internal control—which provides a framework to assist companies in structuring and evaluating controls that address a broad range of risks. Released in 1992 and updated in 2013, 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."[2]

INTERNAL CONTROL OVER FINANCIAL REPORTING

ICFR refers to 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.

ICFR IS ONE ELEMENT OF THE BROADER CONCEPT OF INTERNAL CONTROL.

Misstatements in a financial statement may occur, for example, due to mathematical errors, misapplication of GAAP, or intentional misstatements (fraud). A system of ICFR should address these possibilities. The risk of fraudulent

2 COSO's *Internal Control – Integrated Framework* ©2014 COSO. All rights reserved. Used by permission. See Executive Summary, page 3.

EFFECTIVE ICFR PROVIDES REASONABLE ASSURANCE THAT CORPORATE RECORDS ARE NOT INTENTIONALLY OR UNINTENTIONALLY MISSTATED.

financial reporting is a key consideration in the design and operation of public company ICFR. For example, market expectations for revenues, earnings, or other targets may create pressures on management to meet these thresholds. Effective ICFR provides reasonable assurance that corporate records are not purposefully misstated in response to those pressures. ICFR should therefore be designed and implemented with the risk of fraud in mind and tailored to the particular circumstances of the company.

Financial reporting often requires sophisticated decision making and the application of informed judgment. The following three items, for example, all require management to make judgments regarding assumptions and the likelihood of future events:

- accounting areas such as estimating allowances for credit losses,
- valuing illiquid securities, and
- determining whether intangible assets are impaired.

In these kinds of reporting areas, there is typically a range of acceptable outcomes, rather than a single "correct" result to be measured and recorded. Controls cannot remove the need for judgment or eliminate the variations in reporting inherent in situations in which a range of

THE COSO FRAMEWORK'S FIVE INTEGRATED COMPONENTS OF INTERNAL CONTROL[3]

1. **Control Environment** — The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control, including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

2. **Risk Assessment** — Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of the objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed.

   A precondition to risk assessment is the establishment of objectives, linked

Continued on page 6

3 COSO's *Internal Control – Integrated Framework* ©2014 COSO. All rights reserved. Used by permission. See Executive Summary, pages 4-5.

THE COSO FRAMEWORK'S FIVE INTEGRATED COMPONENTS OF INTERNAL CONTROL

Continued from page 5

at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

3. **Control Activities** — Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

4. **Information and Communication** — Information is necessary for the entity to carry out internal control responsibilities to support the achievement of objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information, and provides information to external parties in response to requirements and expectations.

5. **Monitoring Activities** — Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting bodies or management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate.

acceptable judgments is possible. Controls can, however, be designed and implemented to address the process by which accounting judgments are made and thereby provide reasonable assurance that the financial reports are presented in accordance with GAAP.

REASONABLE ASSURANCE

No system of ICFR can provide absolute assurance that the financial statements are free of misstatements. Internal control systems are operated by individuals, and individuals make mistakes. Further, while maintaining a system of ICFR that provides reasonable assurance regarding the reliability of financial reporting is a legal requirement for most public companies, cost considerations may affect the design of control systems. For these reasons, it is impossible to create a control system that will prevent or detect, on a timely basis, all potential misstatements. 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 standards, processes, and 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 actions established through 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. The following concepts are helpful to understanding control activities:

1. segregation of duties,

2. information technology (IT) general controls,

THE SEC'S DEFINITION OF ICFR

The US Securities and Exchange Commission (SEC or Commission) rules define ICFR as "a process designed by, or under the supervision of, the registrant'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 registrant;

(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 registrant are being made only in accordance with authorizations of management and directors of the registrant; and

(3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the registrant's assets that could have a material effect on the financial statements."[4]

3. entity-level and process-level controls, and

4. preventive and detective controls.

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

4 Securities Exchange Act Rule 13a-15(f).

NO SYSTEM OF ICFR CAN PROVIDE ABSOLUTE ASSURANCE.

process to different persons so that no *one* person can control elements of the process that can be conflicting. 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 related to the accounting for a transaction.

A good example of segregation of duties is assigning responsibility for physical access to a supply room to a person different from the individual who is responsible for maintaining the records of the supplies inventory.

IT General Controls

A company's use of IT affects the manner in which the information relevant to financial reporting is processed, stored, and communicated—and therefore affects the manner in which the system of internal control relevant to financial reporting is designed and implemented. Each component of internal control may involve some extent of automation. The understanding of internal control relevant to financial reporting involves understanding the company's use of IT for each component. The company's use of IT applications or other aspects in the IT environment may result in risks arising from the use of IT.

These risks vary based on whether—and the extent to which—a company relies on IT to support the processes in its information system, to maintain the completeness and accuracy of the underlying data and information, and to support the reliability of automated controls and system-generated reports. IT general controls are typically implemented to address these risks arising from IT.

IT general controls generally include controls in information security, application development, and systems maintenance and operations.

CONTROLS AND SERVICE ORGANIZATIONS

In addition to internally developed controls, management should take into account any relevant controls existing at a service organization that impact ICFR.[5] Companies often outsource important aspects of their business activities to service organizations. Services provided by such organizations become relevant in the context of auditing ICFR when those services and the controls over them affect the company's information system, including related business processes, relevant to financial reporting. Management should obtain an understanding of the nature and significance of the services provided by the service organization and assess the effect of such services on the company's internal control framework.

If an entity determines a service organization is relevant to its financial reporting, the entity can develop and implement its own controls over the services provided by that organization.

Alternatively, the service organization may engage a service auditor to report on the description and design of its controls (type 1 report) or on the description and design of its controls and their operating effectiveness (type 2 report). Such a report may be used by the entity to determine if appropriate controls have been designed and implemented at the service organization to mitigate relevant risks.[6]

5 As defined by PCAOB Auditing Standard 2601, *Consideration of an Entity's Use of a Service Organization* (AS 2601), paragraph .02, a service organization is an entity (or segment of an entity) that provides services to a user organization that are part of the user organization's information system. For example, an entity may outsource its payroll function to an external service organization.

6 AS 2601 provides audit requirements related to an entity's use of a service organization.

As part of risk-assessment procedures, external auditors identify and assess risks arising from IT, including certain cybersecurity risks facing the entity. Relevant controls, including IT general controls, are identified to address these risks. These IT general controls relate to the applications and infrastructures that are relevant to ICFR, including certain cybersecurity controls.[7]

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. Certain entity-level controls have a pervasive effect on the company's system of internal control. Audit committee oversight of financial reporting and a chief financial officer'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. These controls pertain to a single activity, such as requiring that delivery receipts be matched with vendor invoices before a vendor payment is authorized.

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. These controls can be either manual or automated. Here are some examples:

- **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. User access to IT systems should be granted at a level commensurate with job responsibilities, taking into account appropriate segregation of duties, and actively monitored.
- **Automated Controls** — Automated controls include those such as processing controls, and automated calculations, authorization, and approvals.

Detective controls are intended to identify misstatements or unauthorized activities after they have occurred so that corrections can be made in a timely manner. Here are two examples:

- **Reconciliations** — Independently comparing two sets of records that relate to the same transaction

INFORMATION PRODUCED BY THE ENTITY (IPE)

IPE underlies both the processing of financial information as well as the operation of certain internal controls. The Information and Communication component of COSO offers suggested procedures to address the accuracy and completeness of such information. These procedures typically include consideration of source data, report logic, and user-defined parameters used to generate reports.

THE DESIGN, IMPLEMENTATION, AND EVALUATION OF CONTROLS NEED TO BE TAILORED TO THE REPORTING RISKS OF THE COMPANY.

7 See the CAQ's resource, *Understanding Cybersecurity and the External Audit* (February 2016).

THE HIERARCHY OF ICFR DEFICIENCIES

Material Weakness: A material weakness is a deficiency, or a combination of deficiencies, in ICFR, 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.[8]

Significant Deficiency: A significant deficiency is a deficiency, or a combination of deficiencies, in ICFR 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.[9]

Deficiency: A deficiency in ICFR 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.[10]

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.

+ **Management Review Controls (MRCs)** — These controls typically involve comparing recorded financial statement amounts to expected amounts and investigating significant differences from expectations. Such management reviews may include (1) monthly comparison of actual results to forecasted or budgeted results; (2) comparisons of other metrics, such as gross profit margins and expenses as a percentage of sales; or (3) quarterly balance sheet reviews. Examining unexpected deviations might uncover misstatements or unanticipated changes in business activities. When relying on MRCs as part of management's ICFR assessment, it is important to consider whether the control adequately addresses the assessed risks of material misstatement of the significant account or disclosure.[11]

Many MRCs are entity-level controls that vary in nature and precision. An entity-level control may operate at an adequate level of precision to prevent or detect misstatements in a timely manner on its own,[12,13] or may operate in combination with other controls. Factors that can affect the level of precision of an entity-level control and should be considered when assessing the effectiveness of such controls include the (1) objective of the review, (2) level of aggregation of the information subject to review, (3) consistency of performance, (4) correlation to relevant assertions, (5) predictability of expectations, and (6) criteria for investigation.[14]

MRCs may be dependent on other controls, such as those over the processes to populate, update, and maintain the accuracy, completeness, and validity of the information used in the MRC such that the underlying information is sufficiently reliable for its purpose.

8 Regulation S-X Rule 1-02(a)(4) and AS 2201.A7.

9 Regulation S-X Rule 1-02(a)(4) and AS 2201.A11.

10 AS 2201.A3.

11 On October 24, 2013, the Public Company Accounting Oversight Board (PCAOB) issued Staff Audit Practice Alert No. 11 (SAPA No. 11), *Considerations for Audit of Internal Control Over Financial Reporting*. While this alert is directed at external auditors, all stakeholders may benefit from the guidance, including testing management review controls.

12 AS 2201, *An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements*, paragraph .23.

13 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 2007) and AS 2201.23.

14 PCAOB SAPA No. 11, page 20.

SCALING ICFR TO THE COMPANY

The design, implementation, and evaluation of controls need to be tailored to the reporting risks of the company. These risks may be influenced by the size 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 companies may face challenges as a result of limitations in qualified resources.

The risk of management override of controls can be greater in a smaller company in which 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.

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 material weaknesses.

The determination as to whether a deficiency in ICFR represents a material weakness depends on

1. the likelihood of a misstatement occurring as a result of the deficiency;

2. whether the magnitude of the potential misstatement that is reasonably possible to have occurred or could occur in the future as a result of the deficiency, was or could be material to the financial statements; and

3. whether management's controls in the ordinary course of business would have timely prevented or detected a misstatement had it become material.

For the 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 (individually or in the aggregate) of the company's interim or annual 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. •

ICFR ROLES AND RESPONSIBILITIES

MANAGEMENT

Management of the company is responsible for the design, implementation, and monitoring of ICFR. While management structures vary, in many companies, the principal financial officer (the chief financial officer or the chief accounting officer) and his or her staff have day-to-day responsibility for ICFR.

SOX Section 404(a) requires (with certain exceptions) principal executive and financial officers of all public companies to annually assess the effectiveness of ICFR. The SEC has published guidance stating, "Management is responsible for maintaining a system of ICFR that provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles." Further, the SEC guidance states, "Management is responsible for maintaining evidential matter, including documentation, to provide reasonable support for its assessment. This evidence will also allow a third party, such as the company's external auditor, to consider the work performed by management."[15]

IT IS IMPORTANT THAT COMPETENT, WELL-TRAINED INDIVIDUALS ARE INVOLVED IN THE DESIGN AND OVERSIGHT OF ICFR.

In performing its assessment, management must determine whether it has implemented

15 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 2007).

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.[16]

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 system of internal control.

MANAGEMENT REPORTING ON THE EFFECTIVENESS OF ICFR

SOX Section 404(a) also requires (with certain exceptions) all public companies to annually assess the effectiveness of ICFR and report the results. Management is required, in its quarterly reports, to state its responsibility for establishing and maintaining ICFR and disclose any changes to ICFR that have materially affected, or are reasonably likely to materially affect, the company's ICFR.[17] 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.

INDEPENDENT AUDITORS

Section 404(b) of SOX requires most large public companies to have their independent auditor report on the effectiveness of ICFR. Under AS 2201, 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, which includes evaluating the design of controls that are relevant to the audit and determining whether the controls have been implemented. While the auditor is not required to test the operating effectiveness of internal controls, the auditor is required to communicate, in writing to management and the audit committee, material weaknesses or significant deficiencies in the controls that come to his or her attention.

AUDIT COMMITTEES

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 often is delegated to the audit committee, which has specific responsibility for overseeing financial reporting under SOX.

The audit committee's activities usually include

- review of the assessment of financial reporting risks,
- review of management's planned responses to the identified financial reporting risks,

16 AS 2201.29 includes risk factors relevant to the identification of significant accounts and disclosures and their relevant assertions.

17 SOX Section 302 and 906; Regulation S-K, Item 308(c).

- discussion with management of control deficiencies[18] 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 SOX, 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 PCAOB's auditing standards require that the auditor communicate to the audit committee, among other things, an overview of the audit strategy, which typically includes a discussion of ICFR based on the auditor's audit planning work.[19]

WHICH 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 independent registered public accounting firm on the effectiveness of the company's ICFR. Several types of companies, however, are exempt from this requirement. These exempt companies include the following:

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.[20]

Non-Accelerated Filers — Non-accelerated filers are companies that (1) file reports with the SEC and (2) have a public float (i.e., securities available for public trading) of less than $75 million. They are not subject to the same filing deadlines as larger (accelerated) filers.[21]

Emerging-Growth Companies — During the five years following its first registered public sale of common stock, a company that has total annual revenues of less than $1 billion is an emerging growth company (EGC).[22] 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.

18 The auditor is required to communicate to the audit committee in writing all material weaknesses and significant deficiencies identified during the integrated audit (AS 2201.78 and .80) and audit of financial statements (AS 1305, *Communications about Control Deficiencies in an Audit of Financial Statements*, paragraph .04). Auditors also should communicate to management, in writing, all internal control deficiencies identified in ICFR during the integrated audit (AS 2201.81).

19 AS 1301, *Communications with Audit Committees.*

20 SOX Section 405 exempts investment companies registered under Section 8 of the Investment Company Act of 1940 from the requirements of SOX Section 404.

21 Title IX of the Dodd-Frank Act, Section 989G amended SOX 404(b) such that it does not apply to non-accelerated filers.

22 The EGC threshold is indexed to inflation. See https://www.sec.gov/rules/final/2017/33-10332.pdf. For more information about emerging growth companies, see https://www.sec.gov/smallbusiness/goingpublic/EGC.

WHAT ICFR MEANS FOR COMPANIES, INVESTORS, AND MARKETS

Investor confidence and the efficient operation of our capital markets depend on reliable public company financial reporting. An ample body of evidence shows how SOX provisions, including Section 404, have strengthened US capital markets and the reliability of financial reporting.[23] For example:

- A study in a 2017 issue of *Auditing: A Journal of Practice & Theory* concluded that Section 404(b) of SOX provides "an early warning system" for company fraud.[24]
- A 2014 study of the seven-year period from 2007-2013 found that companies subject to 404(b) experienced higher valuation premiums and higher credit ratings (which results in overall lower costs of debt).[25]
- A 2013 Government Accountability Office study found that 80 percent of all companies viewed auditor attestation under Section 404(b) as beneficial to the quality of the company's controls.[26] The risk of material weakness may

AN AMPLE BODY OF EVIDENCE SHOWS HOW SOX PROVISIONS HAVE STRENGTHENED US CAPITAL MARKETS AND THE RELIABILITY OF FINANCIAL REPORTING.

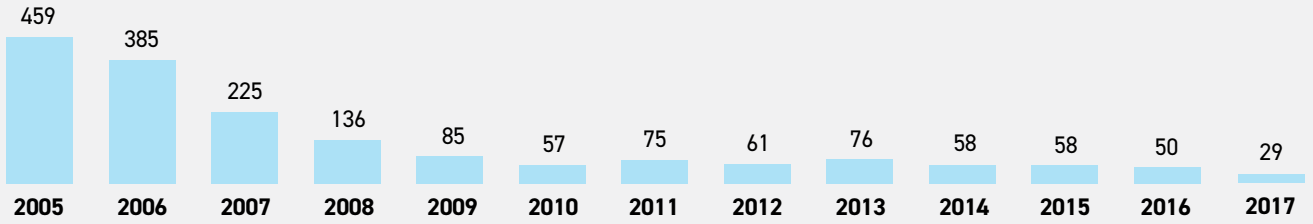
23 The CAQ's *2018 Main Street Investor Survey* found that 78 percent of investors showed confidence in investing in US publicly traded companies and 81 percent of investors showed confidence in public company auditors.

24 See CFO.com, "Research Refutes Sarbanes-Oxley Critics."

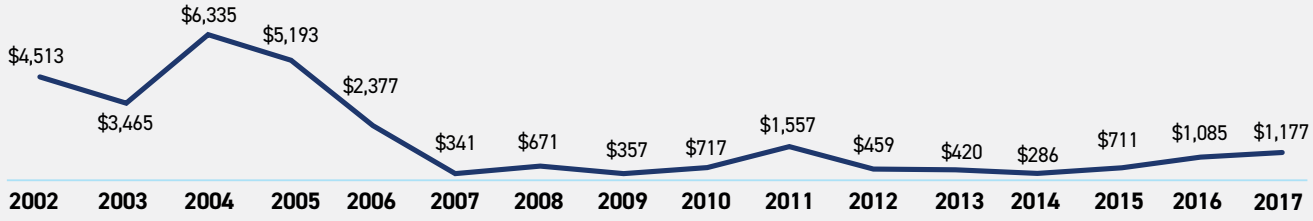
25 See *An Analysis of the Costs and Benefits of Auditor Attestation of Internal Control Over Financial Reporting* (October 2014).

26 See United States Government Accountability Office Report to Congressional Committees, *Internal Controls SEC Should Consider Requiring Companies to Disclose Whether They Obtained an Auditor Attestation*, page 25 (July 2013).

REISSUANCE RESTATEMENTS FROM US ACCELERATED FILERS
Restatements with Form 8-K, Item 4.02



LARGEST NEGATIVE RESTATEMENTS
US$ in millions



Source: Audit Analytics, 2017 Financial Restatements – A Seventeen Year Comparison

be higher among smaller companies. The independent audit of ICFR helps illuminate problems before they lead to material weaknesses and financial restatements, and companies that are not required to comply with 404(b) experience financial reporting problems at a higher rate.[27] Therefore, investors benefit from the discipline and rigor instilled by the requirements to maintain and have an independent evaluation of ICFR.

- A 2009 study analyzed restatements disclosed by two types of SOX 404 issuers (those that had an ICFR audit and those that did not).[28] The study found that companies that disclosed that their ICFR was effective and ***did not*** have an external audit of ICFR under 404(b) had a 46 percent higher restatement rate than companies that disclosed that ICFR was effective and that did have an audit of ICFR.

Enhanced focus on ICFR may have driven a decrease in the number and severity of financial statement restatements since the SOX ICFR requirement became effective in 2004. As illustrated above, the number of reissuance restatements for accelerated filers dropped significantly since 2005 and has maintained a low rate in recent years.[29]

27 Audit Analytics, *2017 Financial Restatements: A Seventeen Year Comparison* (May 2018).

28 *Restatements Disclosed by the Two Types of SOX 404 Issuers – (1) Auditor Attestations Filers and (2) Management-Only Report Filers; Audit Analytics (December 2009),* http://www.alacrastore.com/storecontent/Audit-Analytics-Trend-Reports/Restatements-by-SOX-404-Issuers-2033-14.

29 See EY, *The Sarbanes-Oxley Act at 15*, https://www.ey.com/Publication/vwLUAssets/ey-the-sarbanes-oxley-acts-at-15/$File/ey-the-sarbanes-oxley-act-at-15.pdf.

MORE ICFR RESOURCES

COSO, *Internal Control – Integrated Framework* (2013)

COSO, *Internal Control – Integrated Framework: Executive Summary* (2013)

COSO, *Internal Control – Integrated Framework: Internal Control Over Financial Reporting: A Compendium of Approaches and Examples* (2013)

PCAOB Staff Audit Practice Alert No. 11, *Considerations for Audit of Internal Control Over Financial Reporting*

PCAOB, *Auditing Standard 2201, An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements*

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)

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)

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)


WE WANT
TO HEAR
FROM YOU
So that we can provide resources that are informative and best address the needs of our stakeholders, we would appreciate your response to three short questions.
CLICK FOR SURVEY
SURVEY LINK: http://thecaq.qualtrics.com/jfe/form/SV_37qFxfqEFuLwjgF

GUIDE TO
INTERNA
CONTRO
FINANCIA
REPORTI

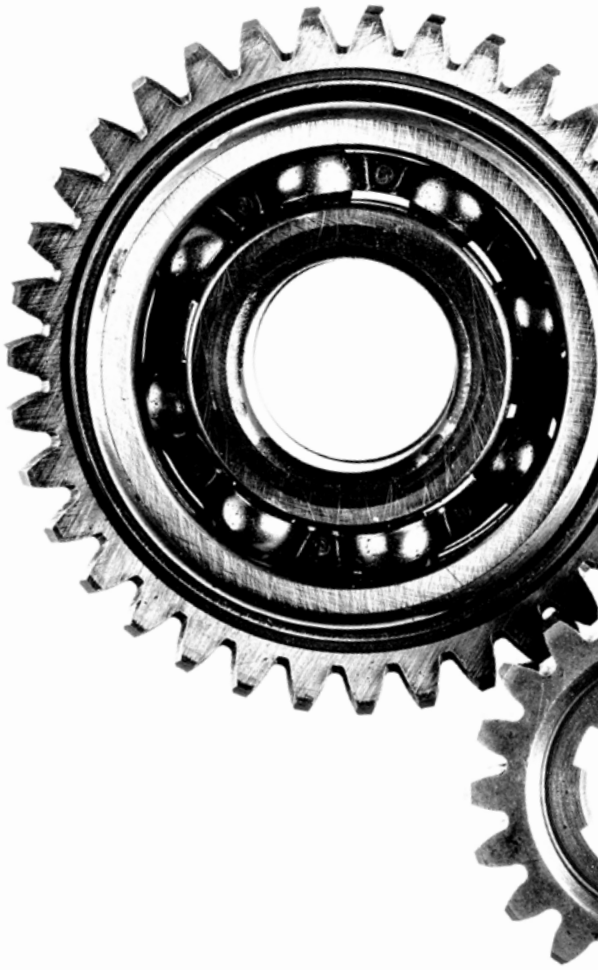
D

AL

L OVER

AL

NG



Published May 2019

THECAQ.ORG

WE WELCOME YOUR FEEDBACK

Please send comments or questions to info@thecaq.org