CHAPTER ONE

1 Background on Internal Controls

THE GOALS AND CHALLENGES OF INTERNAL CONTROLS

The success of an internal controls program is dependent upon ongoing management commitment as an operating requirement that is measured with the operating unit held accountable. As important as an internal control structure is to an organization, an effective system is not a guarantee that the organization will be successful. An effective internal control structure will keep the right people informed about the organization's progress (or lack of progress) in achieving its objectives, but it cannot turn a poor manager into a good one.

Even effective internal control can only help an entity achieve these objectives. It can provide management information about the entity's progress toward their achievement of business goals. However, internal control cannot change an inherently poor manager into a good one. In addition, shifts in government policy or programs, competitors' actions, or economic conditions can be beyond management's control. Internal control cannot ensure success, or even survival.

Internal control is not an absolute assurance to management and the board about the organization's achievement of its objectives. It can only provide reasonable assurance due to limitations inherent in all internal control systems.

For example, breakdowns in the internal control structure can occur due to a simple error or mistake, as well as faulty judgments that could be made at any level of management. In addition, controls can be circumvented by collusion or by management override and a fraudulent payment.

Finally, the design of the internal control system is a function of the resources available, meaning that a cost-benefit analysis must be in the design of the system. The cost of payment controls should never exceed the benefits of the internal system. And the value of a good internal control system should always adequately reduce and help to mitigate risk for the corporate payment process.

Risk-Based Internal Controls

Many companies have ineffective internal controls programs due to an overwhelming amount of controls that don't adequately consider risk. These organizations are only focused on testing the controls and not properly evaluating the effectiveness of the control when conducting a self-assessment or preparing for the annual SOX 404 internal controls assessment process.

A risk-based controls approach properly leverages resources and can reduce the cost of an overall internal controls program and, more importantly, this approach ensures that the control properly mitigates the risk. Risk-based controls focus on the key controls that will mitigate risk within the business process. Failing to take a true risk-based approach may result in identifying more controls than the operation needs. The operation may erroneously focus on perceived "key controls" that do not properly address the risk for a specific business process.

All companies, regardless of size, structure, nature, or industry, encounter risks at all levels within their organization. Risks affect each company's ability to survive, successfully compete within its industry, maintain financial strength and positive public image, and maintain the overall quality of its products, services, and people. Since there is no practical way to reduce risk to zero, management should determine how much risk should be prudently accepted, and strive to maintain risk within acceptable levels by considering the implementation of risk-based controls.

Risk is exposure to a potential loss as a consequence of uncertainty. There are global risks and risks in every phase and stage of a business process, with certain risks of greater importance during each stage. Understanding the types of risk faced within each process sets the foundation for the development of risk-based controls.

As an additional reference, here are ten tips for implementing risk-based controls:

1. The focus should be on the business process and any sub-processes rather than just the audit process.
2. The control should be focused on the end-to-end process and its dependencies rather than just on transactions. Although the control should address the accuracy of a transaction, a risk-based control addresses the total business process and not just a single transaction.
3. The expected outcome is to identify and mitigate risk as well as determine opportunities for process improvements within the operation.
4. There should be a focus on risk management rather than solely on current policies and procedures. Current policies and procedures may be outdated or incorrect.
5. The goal should be on continual risk assessment coverage through a continuous controls monitoring (CCM) process.
6. Risk-based internal controls facilitate change since they should be updated when there is a significant change to the business process or if the control is found to inadequately mitigate a potential risk.
7. This approach should set the foundation for implementing operational metrics and analytics.
8. Risk-based controls can identify risks and business process gaps across financial operations.
9. Risk-based controls can help prevent and detect fraud since they should represent the end-to-end business process.
10. Risk-based controls should always be developed by the business process owners, but approved by management with well-defined implementation and remediation plans.

Here are five questions to ask when developing a series of risk-based controls along with the five key metrics to consider when measuring results.

Five Questions to Ask

1. Does the control consider a failure that may rise to the level of a material weakness?
2. Can the control be relied upon to either prevent or detect (in a timely manner) a material misstatement of the filed financial statements?
3. Has the control been updated recently to reflect the current business process?

4. Has your organization considered remediation actions resulting from a fraudulent activity, findings from external and internal audits, and other control self-assessment processes?
5. Is the control a key component of your continuous controls monitoring (CCM) initiative?

Five Metrics to Consider

1. Number of incidents per period
2. Average value of incidences identified per period
3. Estimate of total value of incidences identified per period
4. Average hourly rate of person remediating incidents per period
5. Percentage of transactions tested per period

Application of Internal Controls

Internal controls should be applied within an operating unit of a corporation in an effective and efficient manner and provide reasonable assurance that the operating unit and corresponding business process will meet its objectives.

Internal control objectives are achieved through the competence and integrity of personnel, the independence of their assigned function, their understanding of prescribed procedures, and the effectiveness of monitoring accepted risk.

The effectiveness of an internal controls system is dependent upon the following factors:

- Senior management commitment and communication
  - The tone set by senior management is the most important factor contributing to the ongoing success of the internal controls system. This is referred to as the "tone at the top" and is supported by a corporate's code of conduct.
- Managers and employees understanding the internal control system along with their responsibilities as business process owners
  - Internal controls should be understood, supported, and promoted throughout the company. This is accomplished by formal training and communication programs for each corporate process.
- Appropriate method of communication
  - Coordination and cooperation among employees is a key dependency. Impediments to necessary communication should be minimized.

- Adequate time and resources
  - Business operations need sufficient time and resources to create, maintain, and review internal controls.

Key Point: A company needs internal controls to ensure business is conducted in accordance with applicable laws and regulations and management's directives and authorities. Effective internal controls will support the company in achieving the goals of minimizing exposure to loss of integrity in operations and financial records, including:

- Loss of assets
- Undetected errors
- Compromise of proprietary data, etc.
- Managing identified risks down to acceptable levels
- Providing the company with disciplined process management
- Facilitating achieving business objectives effectively and efficiently

Key Point: Some of the root causes for internal control problems are listed below.

- The need for controls not recognized throughout the organization
- Inadequate instruction/training
- Insufficient capital or human resources provided to support the controls initiative
- Improper priorities assigned
- Attitudes of employees, supervisors, and managers
- Human error
- Management unaware or not informed of problems within business processes
- Supervisors not monitoring ongoing process

The Three Critical Corporate Controls

The three most critical internal controls for any company can be established by corporate policies that should be "operationalized" into your company's business processes and monitored by the applicable internal control programs. The implementation of these controls set the foundation for good payment controls and risk mitigation. These controls are: (1) segregation of duties, (2) systems access, and (3) delegation of authority. Many companies have

implemented these controls as "core controls" but need to keep them updated by following some of the best practices that are recommended below. The three critical controls will be referenced throughout the standards of internal control provided in this toolkit.

1. **The Segregation of Duties (SoD)** control is one of the most important controls that your company can have. Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will remain undetected by providing for separate processing by different individuals at various stages of a transaction and for independent reviews of the work performed.

   The SoD control provides four primary benefits: (1) the risk of a deliberate fraud is mitigated as the collusion of two or more persons would be required in order to circumvent controls; (2) the risk of legitimate errors is mitigated as the likelihood of detection is increased; (3) the cost of corrective actions is mitigated as errors are generally detected earlier in their lifecycle; and (4) the organization's reputation for integrity and quality is enhanced through a system of checks and balances.

   Although SoD is a basic, key internal control, it is one of the most difficult to accomplish, often due to limited headcount, broadly defined responsibilities, and constantly changing responsibilities. Basically, the general duties to be segregated are: planning/initiation, authorization, custody of assets, and recording or reporting of transactions. Additionally, control tasks such as review, audit, and reconcile should not be performed by the same individual responsible for recording or reporting the transaction.

   Best Practice: Among the most common root causes of fraud are the lack of SoD controls, weak SoD controls, inappropriate compensating controls, or failure to update SoD controls when responsibilities change. As a best practice, many organizations review their SoD controls on a quarterly basis, and whenever staff turnover occurs, as part of their control self-assessment (CSA) process. As a result of this review, the applicable SoD controls are updated appropriately.
2. **System Access:** The principle of SoD in an information system environment is also critical as it ensures the separation of different functions such as transaction entry, online approval of the transactions, master file initiation, master file maintenance, system access rights, and the review of transactions.

In the context of application level controls, this means that one individual should only have access rights which permit them to enter, approve, or review transactions, but no combination of two for the same transaction. Therefore, assigning different security profiles to various individuals supports the principle of SoD. As an example, operational or process SoD within an AP department will determine the system access rights that should be granted for each associate based on roles and responsibilities.

Best Practice: System access rights are reviewed on a periodic basis (usually monthly or quarterly) to ensure that system access capabilities are appropriate for current staff members and reflect any changes in responsibilities or movements to other departments.

3. **Delegation of Authority (DoA):** The last critical control for your company is the DoA policy and control. The purpose of the DoA is to ensure the efficient operation of the company while maintaining fiscal integrity and adherence to policy. Accountability for the overall management of the property, assets, financial, and human resources of the company rests with the chief executive officer (CEO). In many cases the governance of the DoA is the responsibility of the controller. Individuals that have been assigned authority under the terms of the DoA must safeguard company resources by establishing and maintaining internal controls that deter and detect any potential misuse of resources.

   Best Practice: Many companies assign levels of authority to the job grades or levels within the organization and apply workflow to streamline the approval process. If an individual is promoted or moves to another department, his or her level of authority is automatically updated in the employee master file.

The Background and History of Internal Controls

The idea of internal controls is nothing new. In fact, it dates back to ancient civilizations as early as the thirteenth century. It was not until the signing of the Security and Exchange Commission (SEC) Acts of 1933 and 1934, however, that a form of internal control was mandated in the United States. At this point, organizations were officially put on the path to corporate accountability by mitigating risk as a result of better, more effective internal controls. This chapter reviews various milestones, requirements, obstacles, and key events along the way.

Securities Act of 1933

When the stock market crashed in 1929 and billions of investor dollars disappeared, the public lost faith in the capital markets and the United States fell into the Great Depression. In search of solutions, Congress held hearings that resulted in passing the Securities Act of 1933, commonly called the "truth in securities" law. This law required that investors be provided important information about securities for public sale and prohibited fraudulent activity in the sale of securities, such as insider trading. It mandated that securities, with the exception of those exempt, be registered and that related financial information is disclosed.

Securities Exchange Act of 1934

With the passing of the Securities Exchange Act of 1934, Congress created the Securities and Exchange Commission (SEC) and gave it authority over all aspects of the securities industry. The Act granted the SEC disciplinary powers and the authority to mandate reporting, disclosures, and registration of regulated entities. The Securities Act of 1933 and the Securities Exchange Act of 1934 put into place a mechanism for monitoring the securities industry to ensure that companies taking investment dollars tell the truth, are transparent about the risks, and safeguard the interests of their stakeholders.

Trust Indenture Act of 1939

Designed to prevent fraud by providing full and fair disclosure of the character of securities sold in interstate and foreign commerce and through the mails, the Trust Indenture Act of 1939 applies to debt securities offered for public sale. It requires those who issue bonds and the bondholder to enter into a formal agreement in conformance with the standards laid out in the Act.

Investment Company Act of 1940

This law requires companies that offer securities to the public and engage primarily in investing and trading to disclose to the public their financial standing, structure and operations, and investment policies. Although the Act does not permit the SEC to directly supervise the actions of the companies, it is designed to minimize conflicts of interest in complex operations.

Investment Advisors Act of 1940

This act, which was amended in 1996, protects investors by requiring certain financial advisors to register with the SEC. Firms and individuals affected by the regulation are those who manage assets of at least $25 million or who advise registered investment company clients about securities.

Foreign Corrupt Practices Act (FCPA) of 1977

As a result of American corporations having made improper payment to government officials in a number of countries, Congress passed the Foreign Corrupt Practices Act of 1977 in an effort to eliminate such payments to foreign governments, politicians, and political parties, and to restore the reputation of American business. This law generally applies to U.S. corporations, partnerships, and other businesses and persons acting on their behalf, and prohibits any payment, offer of payment, or promise of giving anything of value to a foreign official in an attempt to obtain business.

In addition to its anti-bribery provisions, the law includes broad accounting and recordkeeping rules for companies required to file financial reports. The FCPA requires the companies to maintain toolkits, records, and accounts that accurately reflect the company's transactions and dispositions. Violations of the FCPA by a company and its employees can result in stiff penalties and imprisonment as evidenced by the recent well-publicized Wal-Mart case.

Comprehensive Crime Control Act—1984

This act expanded federal powers to seize assets in civil cases. The law included the Sentencing Reform Act provision, which created the U.S. Sentencing Commission, an independent agency in the judicial branch of government. The Sentencing Commission establishes sentencing policies and practices for federal courts, advises Congress and the executive branch in regard to effective and efficient crime policies, and serves as an information resource on federal crime and sentencing issues.

Federal Sentencing Guidelines for Organizations—1991

Following the savings-and-loan crisis of the 1980s, the U.S. Sentencing Commission responded to the public's frustration with the criminal justice system by releasing the Federal Sentencing Guidelines for organizations, which imposed harsh penalties on organizations whose employees or other agents

have committed federal crimes. The guidelines—seven steps for mitigating the risk of such crimes—include implementing compliance standards and procedures, assigning compliance oversight responsibility to high-level personnel, avoiding delegation to individuals prone to commit crimes, providing information and training on standards, establishing systems for monitoring and reporting criminal conduct without fear of reprisal, enforcing standards and assigning responsibility for detecting offenses, and taking all reasonable steps to guard against offenses in the future.

Internal Control—Integrated Framework—1992 and 2013

Landmark guidance that has been embraced all around the world, Internal Control—Integrated Framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

A commission led by James C. Treadway, Jr., then–Executive Vice President and General Counsel, Paine Webber Incorporated and a former Commissioner of the U.S. Securities and Exchange Commission, was set up. This commission was sponsored and funded by five U.S. private-sector organizations made up of the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the National Association of Accountants (now the Institute of Management Accountants [IMA]). These organizations are collectively called the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

The Committee of Sponsoring Organizations was charged by the Treadway Commission to develop an integrated guidance on Internal Control. As a result of this, a framework for designing, implementing, and evaluating internal control for organizations was released.

The COSO Framework was designed to help businesses establish, assess, and enhance their internal control. The importance of *internal control in the operations and financial reporting* of an entity cannot be overemphasized as the existence or the absence of the process determines the quality of output produced in the financial statements. A present and functioning *internal control process* provides the users with a "reasonable assurance" that the amounts presented in the financial statements are accurate and can be relied upon for informed decision making.[1]

[1]Uwadiae, Oduware, "COSO—An Approach to Internal Framework," accessed October 1, 2018, https://www2.deloitte.com/ng/en/pages/audit/articles/financial-reporting/coso-an-approach-to-internal-control-framework.html.

The timeless concepts of the framework are: Internal controls is a process affected by people; it provides reasonable assurance; and it is geared to the achievement of objectives related to operations, compliance, and financial reporting.

The internal control framework consists of five interrelated components of an internal control system:

1. **Control Environment**, which sets the ethical tone of an organization and influences the control consciousness of its people
2. **Risk Assessment**, which identifies and analyzes the risks to achieving objectives, and determines how the risks should be managed
3. **Control Activities**, which are the policies and procedures that help ensure risks are addressed and management directives are carried out
4. **Information and Communication**, which include operational, financial, and compliance-related reports designed to help ensure information flows down, across, and up the organization; and effective communication with stakeholders
5. **Monitoring**, which assesses the quality of the internal control system's performance on an ongoing basis, through separate evaluations, or a combination of both; reports on findings; and helps ensure continuous improvement of the system, organizational efficiencies, and reduced costs

The five components of the COSO model are depicted in the chart below. The COSO model has driven many internal controls systems and Sarbanes-Oxley efforts in the corporate environment.

Component	Principle
Control Environment	1. Demonstrates commitment to integrity and ethical values
	2. Exercises oversight responsibility
	3. Establishes structure, authority, and responsibility
	4. Demonstrates commitment to competence
	5. Enforces accountability
Risk Assessment	6. Specifies relevant objectives
	7. Identifies and analyzes risk
	8. Assess fraud risk
	9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities
	11. Selects and develops general controls over technology
	12. Deploys through policies and procedures

Component	Principle
Information and Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

COSO's Monitoring Guidance

COSO's Monitoring Guidance, which was updated in 2009, builds on two fundamental principles originally established in COSO's 2006 Guidance:

1. Ongoing and/or separate evaluations enable management to determine whether the other components of internal control continue to function over time.
2. Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action and to management and the board as appropriate.

The updated monitoring guidance further suggests that these principles are best achieved through monitoring that is based on three broad elements:

1. Establishing a foundation for monitoring, including (a) a proper tone at the top; (b) an effective organizational structure that assigns monitoring roles to people with appropriate capabilities, objectivity and authority; and (c) a starting point or baseline of known effective internal control from which ongoing monitoring and separate evaluations can be implemented
2. Designing and executing monitoring procedures focused on persuasive information about the operation of key controls that address meaningful risks to organizational objectives
3. Assessing and reporting results, which includes evaluating the severity of any identified deficiencies and reporting the monitoring results to the appropriate personnel and the board for timely action and follow-up if needed

As recommended in COSO's Guidance for Monitoring Internal Control Systems (Published by the AICPA), organizations may select from a wide variety of monitoring procedures, including but not limited to the list below. The monitoring procedures selected along with the skills and the

objectivity of the evaluators of internal controls will establish the roles and responsibilities.

- Periodic evaluation and testing of controls by internal audit
- Continuous monitoring programs built into information systems
- Analysis of, and appropriate follow-up on, operating reports or metrics that might identify anomalies indicative of a control failure
- Supervisory reviews of controls, such as reconciliation reviews as a normal part of processing
- Self-assessments by boards and management regarding the tone they set in the organization and the effectiveness of their oversight functions
- Audit committee inquiries of internal and external auditors
- Quality assurance reviews of the internal audit department

Continued advancements in technology and management techniques ensure that internal control and related monitoring processes will change over time. However, the fundamental concepts of monitoring, as outlined in COSO's Monitoring Guidance, are designed to stand the test of time. The guidance also covers other concepts that are important to effective and efficient monitoring, including:

- The characteristics associated with the objectivity of the evaluator
- The period of time and the circumstances by which an organization can rely on adequately designed indirect information—when used in combination with ongoing or periodic persuasive direct information—to conclude that internal control remains effective
- Determining the sufficiency and suitability of information used in monitoring to ensure that the results can adequately support conclusions about internal control
- Ways in which the organization can make monitoring more efficient without reducing its effectiveness

COBIT—1996

Control Objectives for Information and Related Technology (COBIT) was created in 1996 by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute. COBIT helps management derive the greatest benefit from information technology through appropriate IT governance and control. Its framework delineates processes and control objectives for planning/organization, acquisition/implementation, delivery/support,

and monitoring/evaluation. This framework also focuses on criteria—effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability—resources, and control objectives necessary for successful IT systems. In addition, COBIT provides management guidelines which comprise maturity models, critical success factors, key goal indicators, and key performance indicators.

SysTrust—1999

Jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), SysTrust is a professional service designed to build confidence and garner trust in the systems that support an entity or activity. It allows for measuring reliability in regard to a system's availability, security, integrity, and maintainability. Certified Public Accountants (CPAs) use SysTrust to verify and provide assurance that system controls are operating effectively.

Corporate Frauds—2001–2002

The late 1990s and early 2000s painted a shameful picture of corporate America—a picture of unbridled greed and arrogance with a no-holds-barred approach to personal gains, an absence of corporate integrity and ethics, aggressive engagement in questionable or fraudulent business practices, highly compromised corporate governance, and—not surprising—the demise of public trust. Although the many corporate frauds perpetrated during this time would fill a toolkit on their own, only two will be covered here: Enron and WorldCom.

Prior to its bankruptcy in late 2001, Enron, the organization named "America's Most Innovative Company" by *Fortune* magazine every year from 1996 to 2001, was one of the world's leading electricity, natural gas, pulp and paper, and communications companies. It employed approximately 22,000 workers. In 2000, the same year Enron was on Fortune's "100 Best Companies to Work for in America" list, it claimed revenues of nearly $101 billion. Enron was widely recognized as an exemplary company with excellent long-term pensions, fine benefits, and extremely effective management.

In August 2001, however, financial analyst Daniel Scotto became concerned about the company's practices and warned his investors to sell Enron stocks and bonds. As later became widely known, many of Enron's recorded assets and profits were inflated, or even wholly fraudulent and nonexistent. The company hid debts and losses by setting up inappropriate

"off-balance sheet" entities. Because these debts were not included in the firm's financial statements, Enron looked more profitable to investors than it actually was. To continue the illusion of billions in profits, even though the company was on the edge of collapse, those at the top of the company perpetrated more and more financial deception, which drove Enron's stock to higher levels. At this point, Chief Financial Officer Andrew Fastow and other executives who had manipulated the deals used insider information and traded millions of dollars of the stock, leaving the company in shambles and Enron stockholders with devastating losses.

Not unlike Enron, the story of WorldCom is one of deception and greed of those at the top who used fraudulent practices to mask declining profits. They classified operating expenses as capital expenditures, creating an illusion of financial growth and profitability to drive up the company's stock. In 2002, when Cynthia Cooper, an internal auditor, discovered the questionable accounting practices and uncovered a $3.8 billion fraud, she blew the whistle by reporting her findings to the WorldCom Audit Committee. The accounting fraud perpetrated by WorldCom executives led to the largest bankruptcy in history, and investors lost an estimated $180 billion.

U.S. Sarbanes-Oxley Act of 2002

The U.S. Sarbanes-Oxley Act of 2002 (SOX) was passed in an effort to hold corporate America responsible for its actions and to help rebuild the trust of the public following the various corporate financial reporting scandals of the late 1990s and early 2000s. It changed the requirements for internal control programs, corporate governance, and corporate accountability for publicly traded companies.

Named after its primary architects—Senator Paul Sarbanes (D-Maryland) and Representative Michael Oxley (R-Ohio)—SOX includes mandates for enhanced corporate governance and financial accountability. I had the pleasure of meeting Senator Sarbanes at an International Accounts Payable Professionals Annual Forum in 2007.

In a nutshell, the law addresses:

Summary of Sarbanes-Oxley Requirements

- Management's certification of the accuracy of financial statements, management's responsibility for ensuring and reporting on the effectiveness of the company's internal controls, and the external auditors' attestation to management's assertion of internal controls

Summary of Sarbanes-Oxley Requirements
■ New requirements for corporate boards and audit committees, including enhancing the audit committee's (ACs) oversight responsibility for the financial management of the organization, hiring and overseeing the external auditors, and ensuring that a financial expert is a part of the AC ■ Disclosure of a code of conduct for financial officers, protection of whistleblowers, and accelerated reporting of insider trading ■ Establishment of the independent Public Accounting Oversight Board (PCAOB) as the standard setting body for auditing ■ Criminal penalties for management's issuance of fraudulent financial certifications ■ Reinforcement of the external auditors' independence, ensuring they are not "involved" in the management or implementation of activities they audit; and required five-year rotation of the lead auditor

Key Point: Section 404 requires an annual report by management on the design and effectiveness of internal controls over financial reporting, and an attestation by the company's auditors as to the accuracy of management's assessment:

- Evaluate and test internal controls over financial reporting using COSO to opine on effectiveness (broad and deep).
- Assessment must be based on procedures sufficient to evaluate design and test operating effectiveness. Inquiry alone will not provide adequate basis for assessment.
- Significant support is required from operations and controller organizations as up to 70% of key controls can be outside of financial reporting.

Management's responsibilities include:

- Evaluate design and effectiveness of internal controls over financial reporting.
- Support evaluation with sufficient evidence, including documentation and test results.
- Written assessment of effectiveness of internal controls over financial reporting as of the end of the company's most recent fiscal year.
- Management must maintain evidential matter, including documentation, to provide reasonable support for its assessment and testing of both design and operating effectiveness.

Key Point: Definitions to describe a controls weakness are:

Significant deficiency: A control deficiency, or combination of control deficiencies, that adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the company's annual or interim financial statements that is more than inconsequential will not be prevented or detected.

Material weakness: A significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected. To ensure successful outcome, many organizations have listed the following items as best practices that can be followed by privately held companies:

Sarbanes-Oxley Best Practices

- Have strong steering and disclosure committees.
- Engage the external auditor early.
- Develop organization-wide communications for every annual event.
- Management buy-in is essential with key stakeholders.
- Balance documentation effort and use automation where possible.
- Ensure that company resources and process owners are engaged throughout the process.
- Identify and support champions for keeping information current.
- Develop livable, structured process for updating documentation to conflict organization or system changes.
- Ensure periodic reviews of the organization's internal controls programs.

ENTERPRISE RISK MANAGEMENT (ERM) INTEGRATED FRAMEWORK—2004 AND 2013

COSO defines enterprise risk management (ERM) as a "process, effected by an entity's board of directors, management, and other personnel; applied in strategy setting and across the enterprise; designed to identify potential events that may affect the entity; and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

In the Enterprise Risk Management Integrated Framework, COSO expands its highly acclaimed Internal Control Integrated Framework to more broadly explore and expand risk management from four perspectives: strategic, operational, financial, and compliance. Building upon the internal control framework, the components of the ERM framework include the internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

Example: Enterprise Risk Management (ERM) and the Application to the Procure to Pay (P2P) Cycle

Enterprise risk management (ERM) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring process. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.[2]

ERM can also be described as a risk-based approach to managing an enterprise, integrating concepts of internal control, the Sarbanes-Oxley Act, data protection, and strategic planning. ERM is evolving to address the needs of various stakeholders, who want to understand the broad spectrum of risks facing complex organizations to ensure they are appropriately managed. Regulators and debt rating agencies have increased their scrutiny on the risk management processes of companies.

We have all been focused on implementing internal controls within our organizations in order to meet the requirements of the Sarbanes-Oxley Act (SOX), Section 404. Many companies have asked if their control processes are headed in the right direction, and started to wonder if they are "just going through the motions." Another question to consider: Do the controls adequately address the risk of an organization or entity that is not

[2]Wikipedia, "Enterprise Risk Management," accessed October 2, 2018, https://en.wikipedia.org/wiki/Enterprise_risk_management.

meeting its objectives or accomplishing a key strategy? Lastly, can the risk be managed?

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued *Internal Control—Integrated Framework* to help businesses and other entities assess and enhance their internal control systems. That framework has since been incorporated into policies, rules, and regulations, which are used by thousands of enterprises to better control the process to achieve established objectives.

ERM is a process, affected by an entity's board of directors, management, and other personnel, that is applied during strategy setting across an enterprise in order to:

- Identify potential events that may affect the entity and manage risks to be within its "risk appetite," which can be defined as the risk tolerance that a firm is willing to allow.

  Some firms are very conservative and avoid risk by the focus on too many controls. As an example, a firm may have multiple levels of approvals for expenditure. This can become a signature-gathering process rather than a true approval process.
- Provide reasonable assurance regarding the achievement of entity objectives.

  ERM is a process that provides a reasonable level of assurance that the firm's total objectives will be achieved.

ERM is designed to raise a consistent "risk-and-control consciousness" throughout an enterprise and become a commonly accepted model for discussing and evaluating the risk management process.

ERM consists of eight interrelated components that are developed from the way management runs an enterprise and should be integrated with the management process. The components are:

1. **Internal Environment**—The internal environment encompasses the tone of an organization. It sets the basis for how risk is viewed and addressed, including risk management philosophy, risk appetite, integrity, ethical values, and the environment in which they operate.
2. **Objective Setting**—Objectives must exist before management can identify potential events affecting their achievement. ERM ensures that

management has a process established to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

3. **Event Identification**—Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's *strategy or objective-setting processes*.
4. **Risk Assessment**—Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed.
5. **Risk Response**—Management selects risk responses—avoiding, accepting, reducing, or sharing risk—to develop a set of actions that align risks with the entity's risk tolerance.
6. **Control Activities**—Policies and procedures are established and implemented to help ensure the risk responses are carried out effectively.
7. **Information and Communication**—Relevant information is identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
8. **Monitoring**—The entirety of ERM is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both. Management activities are defined as business planning, internal controls, communication, corporate governance, and corporate infrastructure.

An ERM Checklist

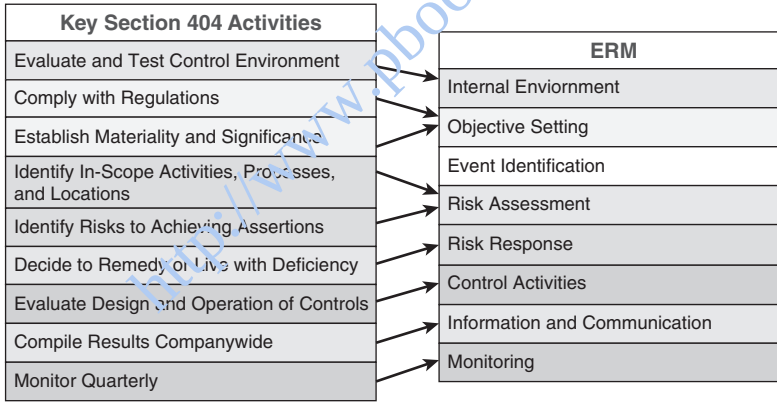
Starting at the enterprise level, control considerations include:

1. **Established and communicated enterprise-level objectives**, including how they are supported by strategic plans and complemented on a process/application level. A risk assessment process, including estimating the significance of risks, assessing the likelihood of their occurrence, and determining needed actions, should be established.
   - Does cthose levels?
   - Are acquisitions and divestitures of significant assets appropriately controlled (e.g. a completed due diligence procedure that has been reviewed by the appropriate level of management)?
   - Are there adequate mechanisms for identifying business risks, including those resulting from:

- New markets or lines of business?
- New products and services?
- Privacy and data protection compliance requirements?
- Other changes in the business, economic, and regulatory environment?

2. **Adequate organization-level communication** to enable people to discharge their responsibilities effectively, allowing management to take timely and appropriate follow-up action on communications received from customers, vendors, regulators, and/or other external parties.
   - Is there a process for tracking communication?
   - Is ownership assigned to specific management personnel to help ensure the entity responds appropriately, timely, and accurately to communications?

Key Point: ERM involves companywide motivation. While ERM is not a regulatory requirement, it can establish a competitive advantage. The diagram below matches key Section 404 activities with the ERM model. As you can see, the ERM model supports and complements the requirements of SOX 404.



Internal Control over Financial Reporting—Guidance for Smaller Public Companies—2006

For years, smaller companies struggled to apply COSO's Internal Control — Integrated Framework. In this guidance, COSO provides a principles-based approach to internal control, uniquely designed for smaller companies. It actually has proved beneficial, however, to companies of all sizes. This guidance

helps management to establish and maintain effective internal control over financial reporting and provides information on complying with new rules and regulations while containing costs.

Guidance on Monitoring Internal Control Systems—2009

Recognizing the absence of available resources on monitoring, COSO released this guidance to help organizations ensure they have an accurate understanding of the effectiveness of their internal controls so that they can take corrective action as warranted. This guidance advocates a proper tone at the top that supports monitoring, an effective organizational structure that assigns monitoring roles to people with appropriate capabilities, objectivity and authority, and a "baseline" at which the monitoring begins and from which accurate conclusions about improvement can be drawn. Other activities include the design and execution of monitoring procedures, assessing and reporting results, and following up as needed.

Definition and Objectives of Internal Controls

Internal controls are desired goals or conditions for a specific event cycle which, if achieved, minimize the potential that waste, loss, unauthorized use, or misappropriation will occur.

For a control objective to be effective, compliance with it must be measurable and observable. The control objectives include authorization, completeness, accuracy, validity, physical safeguards and security, error handling, and segregation of duties and are described below.

- **Authorization.** The objective is to ensure that all transactions are approved by responsible personnel in accordance with specific or general authority before the transaction is recorded.
- **Completeness:** The objective is to ensure that no valid transactions have been omitted from the accounting records.
- **Accuracy:** The objective is to ensure that all valid transactions are accurate, consistent with the originating transaction data, and information is recorded in a timely manner.
- **Validity:** The objective is to ensure that all recorded transactions fairly represent the economic events that actually occurred, are lawful in nature, and have been executed in accordance with management's general authorization.

- **Physical Safeguards and Security:** The objective is to ensure that access to physical assets and information systems is controlled and properly restricted to authorized personnel.
- **Error Handling:** The objective is to ensure that errors detected at any stage of processing receive prompt corrective action and are reported to the appropriate level of management.
- **Segregation of Duties:** The objective is to ensure that duties are assigned to individuals in a manner that ensures that no one individual can control both the recording function and the procedures relative to processing the transaction. As noted, segregation of duties is one of the three critical corporate controls.

Types of Internal Controls and Control Mechanisms

Major Types of Internal Control

There are three main types of internal controls: preventive, detective, and corrective as defined below.

1. **Detective:** Designed to detect errors or irregularities that may have occurred
2. **Corrective:** Designed to correct errors or irregularities that have been detected
3. **Preventive:** Designed to keep errors or irregularities from occurring within the business process

The table below applies the control type to standard risk objectives, and control measures or activities:

Risk Management Objective	*Control Measure*	*Type of Control*
Segregation/ Authorization	■ Physical and logical access control ■ Audit trails	■ Preventive ■ Detective
Accuracy	■ Automatic validation ■ Data verification ■ Application change control ■ Audit trails	■ Preventive ■ Detective or Corrective ■ Preventive ■ Detective
Completeness	■ Application change control ■ Record counts ■ Cross-totals ■ Audit trails	■ Preventive ■ Detective ■ Detective ■ Detective

Risk Management Objective	*Control Measure*	*Type of Control*
Confidentiality	■ Physical and logical access control ■ Audit trails	■ Preventive ■ Detective
Auditability	■ Only access production data through authorized programs ■ Audit trails	■ Preventive ■ Detective
Continuity/ Recovery	■ Backups and recovery plans	■ Corrective

Compensating Controls

Effective compensating controls can improve the design of a process that has inadequate segregations of duties and ultimately provide reasonable assurance to managers that the anticipated objective(s) of a process or a department will be achieved.

However, compensating controls are less desirable than the segregation of duties internal control because compensating controls generally occur after the transaction is complete. Also, it takes more resources to investigate and correct errors and to recover losses than it does to prevent an error.

Other Controls

Other organization and corporate defined controls are described in the following sections. These types of controls are embedded in the governance structure of a corporation and support the major types of controls that are integral to the payments process.

Organization Controls

Organizational controls should cover all aspects of the company's business processes without overlap, and be clearly assigned and communicated.

- Responsibility should be delegated down the level at which the necessary expertise and time exists.
- No single employee should have exclusive knowledge, authority, or control over any significant transaction or group of transactions.
- Agreeing realistic qualitative and quantitative targets strengthens responsibility.

- The structure of accountability depends upon continuing levels of competence of employees in different positions and the development of competence so that responsibility and reporting relationships can be regrouped in more efficient ways.

Policy Controls

Policy controls are the general principles and guides for action that influence decisions. They indicate the limits to choices and the parameters or rules to be followed by the company and its employees. Major policies should be reviewed, approved, and communicated by senior management. Policies are derived by:

- Considering the business environment and process objectives
- Identifying the potential categories of risks that the environment poses toward achievement of the objectives

Procedure Controls

Procedure controls prescribe how actions are to be performed consistent with policies. Procedures should be developed by those who understand the day-to-day actions that will be subject to the procedures.

Supervisory Controls

Examples of supervisory controls are situations in which managers ensure that all employees understand their responsibilities and authorities, and the assurance that procedures are being followed within the operating unit.

Review Controls

Review controls include an ongoing self-assessment process as required by the Sarbanes-Oxley Act of 2002. A controls self-assessment (CSA) process is a series of questions that validate the effectiveness of the control environment. As a best practice, a self-assessment must be conducted every fiscal quarter for a specific business process or sub-process. In some situations, the manager of the operating unit may elect to conduct a self-assessment test more frequently if automated continuous monitoring tools are used. It is imperative that all weaknesses found in the testing process are remediated through a corrective action and follow-up process.

LEVERAGING THE STANDARDS OF INTERNAL CONTROL TO IMPLEMENT A CONTROLS SELF-ASSESSMENT (CSA) PROGRAM

The Institute of Internal Auditors (IIA) defines CSA as a process through which internal control effectiveness is examined with the objective of providing reasonable assurance that all business objectives are met. The employees performing CSA work are in the functional area being examined rather than upper-level managers that are above the system of internal controls.

These employees have a wealth of information about internal controls and fraud (if it exists). While internal (or independent) auditors can be involved with CSA initiatives, auditors do not "own" the process and do not make the assessments and evaluations.

Key Point: If there is an environment of internal control, controls are understood and embedded at the tactical level, and the process is validated by a CSA, cost of controls can be reduced drastically. More importantly, the risk of fraudulent behavior is significantly mitigated. The standards of internal control provided in this toolkit will help to determine the areas of risk and key controls to focus on in a CSA process.

The most common approaches to performing CSA activities are facilitated team meetings, CSA surveys, and management's focus on a specific internal control or area of their business.

- A **facilitated team meeting** is the most popular form of CSA. The facilitated sessions consist of 6 to 15 employees who are subject on a day-to-day basis to the internal controls being evaluated. A trained facilitator guides the meeting, and another individual records the activity.
- The **survey approach** uses questionnaires to elicit data about controls, risks, and processes. It differs from traditional internal control questionnaires used by auditors because the operational employees (not the auditors) use the survey results to self-evaluate the controls or processes. At some companies a survey approach may be used to evaluate "soft" controls. It may be used to evaluate the effectives of an ethics program that is considered an entity-level control. (Refer to Chapter 16.)

The steps below support the self-assessment approach in a CSA program. Self-testing on a regular basis validates the effectiveness and design of the control. This approach can be used when management would like to review

the controls of a specific process. Lastly, this approach can also be used in a workshop setting.

1. **Understand the operating unit or business process.** A key component of a CSA program is ensuring that the control points and responsibilities of the operating unit are understood.
2. **Determine the scope of the CSA initiative.** Clearly define the CSA scope and the controls that will be assessed for a specific business process.
3. **Ensure there is management commitment.** This is crucial to the ongoing support and success of the program. It is demonstrated by full management understanding of the value-added benefits of a CSA program.
4. **Match the CSA program to the operating unit.** Develop a program that represents the operating unit or process or select from the recommendation standards of internal control
5. **Form a CSA team or work team.** Work teams or process teams, with the assistance of a facilitation team, identify obstacles to overcome or strengths to be leveraged and agree upon appropriate action steps to improve the group's effectiveness. As an example, a process-based CSA Team will focus on a process that may only entail one activity of a particular business unit or processes such as procure to pay and accounts payable. Suitable candidates for the CSA tem are:
   - Work teams that work together on a single business process that may cut across functional management boundaries
   - Work teams that are about to implement a new process or application system
   - Teams that tend to be staff-based in that most of those attending should be the individuals performing the work
   - Areas where basic day-to-day processes require improvement
6. **Plan and schedule the evaluation of internal controls.** Although an internal controls program should be flexible to address the changing business environment, a quarterly plan and schedule for the CSA program helps to work around peak periods of activity.
7. **Complete the evaluation of internal controls.**
8. **Develop deficiency findings and remediation activities.** A deficiency finding is a factual statement of a problem without judgment or conclusion and should be quantified where possible. Findings should address the root cause of the problem and identify "what is really broken."
9. **Develop a corrective action plan.** A corrective action plan is an internal controls team and/or management plan that addresses the status

of findings on an ongoing, scheduled basis. The CSA team is responsible for managing the implementation of the corrective action plan. The plan needs to include:

- Finding reference
- Corrective action
- Owner of the individual corrective action. An individual should own the corrective action plan to ensure accountability.
- Commitment date
- Status
- Actual date the correction occurred
- Revised or retesting recommended
- Review of recommended corrective action
- Attached supporting documentation as evidence of completion of the corrective action (e.g. process change, system access issues due to segregation of duties issues corrected)

10. **Follow-up and retest the finding.** Corrected findings need to be verified by following up and retesting the issue by the review of audit trails, process changes, and sampling transactions after the correction took place.
11. **Management reporting and review.** Ongoing management review of internal controls program results indicates the commitment and strengthens the accountability in each organization within the operating unit.
12. **Conduct ongoing training.** Internal controls training is key to the operating unit understanding of internal controls components and requirements and should be provided on an annual basis. Business process owners responsible for the payments process should have specific training programs for new hires if there has been a process change or a new system or solution has been implemented.
13. **Update standards of internal control (key controls).** Standards of internal control supporting the CSA process should be updated to reflect the results of corrective action plans.

ETHICS AND "TONE AT THE TOP"

The connection between fraud and the tone at the top of an organization has received a great deal of attention over the last few years. "Tone at the top" refers to the ethical atmosphere that is created in the workplace by the organization's

leadership. Whatever tone management sets will have a trickle-down effect on employees of the company. If the tone set by managers upholds ethics and integrity, employees will be more inclined to uphold those same values.

As a best practice, many organizations integrate ethics and compliance requirements into all business processes. Companies need to ensure that an environment of ethics and compliance is embedded within their areas of responsibility. Additionally, a business process owner plays a key role in managing all internal control initiatives in private and public companies. These initiatives usually include the deployment of ethical standards or a code of conduct for the organization.

What is "tone at the top"?

The tone at the top establishes the integrity of a company and directs how employees, shareholders, and stakeholders of a company will behave. A tone at the top focused on personal salary and greed, or that supports and overlooks fraudulent activities, results in a company that may behave the same way. A tone at the top that is focused on doing the right thing for employees, shareholders, and stakeholders results in a company that has an environment of openness and honesty.

What are the components of an effective ethics policy?

1. Communicates an organization's ethical values, standards, and commitments to stakeholders that will underpin the way that it does business
2. Confirms leadership commitment to the above
3. Describes how this will be achieved and monitored through an ethics program
4. Identifies the main ethical issues faced by the organization
5. Identifies other policies and documents that support and detail aspects of the ethics policy—such as a code of ethics, a speak-up policy, a bullying and harassment policy, a gifts and hospitality policy, an environment policy, etc.

What are the components of a well-defined code of conduct?

As a best practice, companies and organizations of all sizes have implemented a code of conduct to support their "tone at the top" message. The Institute

of Business Ethics suggests that a code of conduct include the following components:

- How we compete
- Bribery and facilitation payments
- Gifts and entertainment
- Conflicts of interest
- Use of company assets
- Safeguarding important information
- Political involvement and contributions
- The application of human rights standards in our business
- Our environmental responsibilities
- Timely payments of suppliers
- Other issues

What are examples of poor "tone at the top"?

According to the AICPA, the following list provides examples of poor tone at the top and establishes a negative work environment for an employee who is vulnerable to a fraudster. These examples or symptoms also support the Fraud Triangle concept in which there must be: (1) Need, (2) Rationalization, and (3) Opportunity for an individual to commit fraud.

- Top management apparently not caring about or rewarding appropriate behavior
- Lack of recognition for proper job performance
- Negative feedback
- Perceived organizational inequities
- Autocratic management rather than participative management
- Unreasonable budget expectations or other financial targets
- Low organizational loyalty
- Fear of delivering "bad news" to supervisors and/or management
- Less-than-competitive compensation
- Poor training and promotional opportunities
- Unfair, unequal, or unclear organizational responsibilities
- Poor communication practices or methods within the organization

CODE OF CONDUCT CONSIDERATIONS

An environment of internal control in any size organization begins with the tone at the top, which is reflected in the company's code of conduct. A code of conduct establishes the organization's commitment to internal controls, which can help protect the company against fraud. Fraud can occur in organizations of all sizes and in all industries. Controllers and business process owners have the responsibility to ensure that the accounting staff exhibits the highest ethical behavior possible. Negative ethical behavior usually shows up in accounting processes where payments are made, such as accounts payable and payroll.

The following three types of fraud are examples of violations of tone at the top:

1. **Internal fraud:** One or more employees facilitate the activity by using false entries to cover the action. The activity can be concealed for a length of time so that fraud is not easily recognized.
2. **External fraud:** Someone outside of the accounts payable department is able to gain access to company assets through fraudulent means. As a result, funds are misappropriated or extorted from the company.
3. **Conspiracy fraud or collusion.** This is a combination of both internal and external fraud in which an employee conspires with someone outside of the company such as a vendor or an ex-employee to commit a fraudulent activity.

ENTITY-LEVEL CONTROLS

Entity-level controls have a pervasive influence throughout all organizations. If they are weak, inadequate, or nonexistent, they can impact material weaknesses relating to an audit of internal control. Week entity-level controls can also lead to material misstatements in the financial statements of the company. The presence of material misstatements could result in receiving an adverse opinion on internal controls and a qualified opinion on the financial statements.

Entity-level controls should be included in the internal controls programs for all companies and organizations, no matter how large or small. In a January 11, 2010, article, "Taking Control: Public Company Auditors Use Internal Controls to Measure Effectiveness," published by the AICPA's *CPA Insider*, it was noted that entity-level controls (also called top-level controls or management review controls) can provide effectiveness for all controls.

"Entity-level controls are often related to the monitoring process and financial close and reporting cycle—although small companies may not refer to them in those words," explains Wayne Kerr, senior consultant with Thomson Reuters. Kerr says that these top-level controls are items such as weekly or monthly top management reviews of financial information; approval of large transactions, such as payments or sales; and reviews of bank reconciliations.

"Smaller companies rely on these types of controls, in part, because they often lack the resources or capacity to incorporate separation of duties and other 'prevent' controls into their processes," he adds.

Benefits for Entity-Level Controls

There are several benefits to implementing an effective entity-level controls program that are applicable to all types of organizations. These benefits include:

- Reduction of the likelihood of a negative risk event by establishing and reinforcing the infrastructure that sets the control consciousness of the organization.
- For companies conducting evaluations of internal controls, the presence of effective entity-level controls can contribute to a more effective and efficient evaluation strategy.
- Increased effectiveness and efficiency of management's risk assessment and controls evaluation.
- Enforcing the adherence to an internal controls framework.
- An assessment of entity-level controls can highlight potential problems that require a revision of existing internal controls programs at the activity level.

"Tone at the Top"

This is a subjective analysis on the emphasis and seriousness that senior management displays toward internal controls and compliance. This can be

quite easy to determine based on the results of the tests mentioned above, but can also be supported by reviewing the following:

- Has the company implemented the appropriate internal control framework?
- Does the company have the requisite amount of independence in the audit, finance, and other functional areas as evidenced by the organizational chart?
- Are meeting minutes documented for each board of directors meeting?
- Do the CEO and president participate in the follow-through and implementation of internal control reviews, gaps, and remediation? Is this documented?

Depending upon the complexity of the organization, there are additional considerations to include in the evaluation of entity-level controls:

- Controls Over Management Override
- The Company's Risk Assessment Process
- Centralized Processing and Controls, Including Shared Service Environments
- Controls to Monitor Results of Operations
- Controls to Monitor Other Controls, Including Activities of the Internal Audit Function, the Audit Committee, and Self-Assessment Programs
- Controls Over the Period-End Financial Reporting Process
- Policies That Address Significant Business Control and Risk Management Practices
- Internal Audit
- Ethics Hotline
- Code of Conduct
- IT Environment and Organizations
- Self-Assessment
- Disclosure Committee
- Oversight by the Board or Senior Management
- Policies and Procedures Manual
- Variance Analysis Reporting
- Remediation Mechanism
- Management Triggers Embedded Within IT Systems
- Internal Communication and Performance Reporting
- Tone at the Top

- Board and Audit Committee Reporting
- External Communication
- Segregation of Duties
- Account Reconciliations
- System Balancing and Exception Reporting
- Change Management
- Risk Assessment Methodology
- Corporate Governance
- Delegation of Authority Policies
- Hiring and Retention Practices
- Fraud Prevention/Detection Controls and Analytical Procedures

ROLES AND RESPONSIBILITIES FOR INTERNAL CONTROL

Internal control over financial reporting continues to be a major area of importance in the governance of an organization. The table presented in this section was developed to provide a template to suggest the roles and responsibilities for the specific components of an organization's system of internal controls that can be used in both public and privately held companies. The roles and responsibilities include those of the Employees, Board of Directors, Audit Committee, Chief Executive Officer and Executive Management Team, Controller and Chief Financial Officer (CFO), Internal Controls Team, Assertion Team, SOX 404 Steering Committee, Internal Auditors, and External Auditors.

Key Point: Ownership of internal controls is critical for all levels of organization. Management directives must be:

- Developed and documented
- Communicated
- Understood (existence, meaning, and use) by appropriate people
- Supported by processes to ensure compliance
- Supported by management

Responsibilities	Definition of Responsibilities
Employees	■ Employees support the organization's internal control program and adhere to the organization's code of conduct and tone at the top. ■ The internal control system is only as effective as the employees throughout the organization who must comply with it. Employees throughout the organization should understand their role in internal control and the importance of supporting the system through their own actions and encouraging respect for the system by their colleagues throughout the organization.
Audit Committee	■ Boards of directors and audit committees have responsibility for making sure the internal control system within the organization is adequate. ■ This responsibility includes determining the extent to which internal controls are to be evaluated.
Chief Executive Officer (CEO) and Executive Management Team of the Organization	■ The chief executive officer is ultimately responsible and should assume ownership of the system. ■ More than any other individual, the chief executive sets the tone at the top that affects integrity and ethics and other factors of a positive control environment. ■ Senior managers in turn assign responsibility for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions. ■ In a smaller entity, the influence of the chief executive, often an owner-manager, is usually more direct. In any event, in a cascading responsibility, a manager is effectively a chief executive of his or her sphere of responsibility. ■ In a large company, the chief executive fulfills this duty by providing leadership and direction to senior managers and reviewing the way they're controlling the business. ■ As an indication of management's responsibility, top management at a publicly owned organization will include, in the organization's annual financial report to the shareholders, a statement indicating that management has established a system of internal control management believes is effective. The statement may also provide specific details about the organization's internal control system. ■ The primary responsibility for the development and maintenance of internal control rests with an organization's management. With increased significance placed on the control environment, the focus of internal control has changed from policies and procedures to an overriding philosophy and operating style within the organization. ■ Emphasis on these intangible aspects highlights the importance of top management's involvement in the internal control system. If internal control is not a priority for management, then it will not be one for people within the organization, either.

Responsibilities	Definition of Responsibilities
Controller and Chief Financial Officer (CFO)	■ Controllers and CFOs are usually responsible for the development and implementation of internal controls programs for their companies. ■ Controllers and CFOs are also responsible for the results of the effectiveness of the organization's internal controls programs, which means that controls must be updated to reflect current system and operational environments. ■ They are required to ensure that all accounting practices impacting financial results are properly controlled. ■ Controllers and CFOs also drive the assertion process required by Sarbanes-Oxley (SOX) 404. They may lead an Internal Controls Team with Assertion Teams to facilitate this effort as described below. ■ A controller and CFO may also enlist the efforts of a Sarbanes-Oxley (SOX) Steering Committee to help with the governance of the internal controls program and assertion process. This approach is also described below.
Internal Controls Team (Public Company Example)	The VP of Internal Controls, along with the Internal Controls Team, is responsible for implementing the requirements of Sarbanes-Oxley (SOX) 404, by which the organization's internal controls are documented and evaluated. This requirement includes implementing the foundational direction for the organization's internal controls program. Specific responsibilities of the Internal Controls Team include: **Project Management** ■ Primary liaison to impacted organizations and external service providers and escalate project-wide issues to management and Steering Committee for resolution. **Tactical Project Focus** ■ Interact with controls and procedures owners. ■ Ensure delivery of all tasks assigned to the specific work stream. ■ Report to the Internal Controls Project Manager to obtain scope approval. ■ Assist with issue escalation and provide milestone progress updates. ■ Responsible for day-to-day work effort in areas of ownership. ■ Working for the Internal Controls Project Manager, complete assigned workload with designees from control and procedures owners. **Disclosure Committee, Audit Committee, and SEC Reporting (10Q and 10K)** ■ The VP of Internal Controls attends each Disclosure Committee meeting and presents significant controls issues that impact the organization's key controls. ■ The VP of Internal Controls attends each Audit Committee meeting and provides SOX 404 project updates and presents significant control issues. ■ The VP of Internal Controls develops the response for the evaluation of internal controls for the 10Q and 10K reports.

Responsibilities	Definition of Responsibilities
Assertion Team (Public Company Example)	As part of the structure for the SOX 404 project, and to establish the foundational structure control environment, Assertion Teams are established to represent each accounting cycle, process, and/or business area. The Assertion Team is responsible for: ■ Providing input and signoff on the scope of the SOX 404 project ■ Participating in workshops, and providing access to subject matter experts (SMEs) ■ Completing assertion packages with the Internal Controls team ■ Approving deliverables ■ Providing input into testing effort during planning, execution, and results remediation stages ■ Addressing remediation actions ■ Accepting responsibility for ongoing maintenance of controls and documentation
SOX 404 Steering Committee (Public Company Example)	The SOX 404 Steering Committee has the following responsibilities: ■ The SOX 404 Steering Committee will provide written certification to support the organization's Section 404 assertion on internal controls on an annual basis. This effort is supported by the sub-certification process at the detailed process-owner level and the deliverable acceptance in individual process areas. ■ The SOX 404 Steering Committee will review sensitive policies required for SOX 404 compliance, including: Segregation of Duties, Delegation of Authority changes, and remediation and resolution of other enterprise-wide issues. ■ The SOX 404 Steering Committee will provide visible sponsorship of project and commitment of skilled resources from all represented areas, and committee members play an important role in reviewing and understanding the project scope, approach, and risks.
Internal Auditors	■ Internal auditors' responsibilities typically include ensuring the adequacy of the system of internal control, the reliability of data, and the efficient use of the organization's resources. Internal auditors identify control problems and develop solutions for improving and strengthening internal controls. ■ Internal auditors are concerned with the entire range of an organization's internal controls, including operational, financial, and compliance controls.
External Auditors	■ Internal controls will also be evaluated by the external auditors. External auditors assess the effectiveness of internal control within an organization to plan the financial statement audit. ■ In contrast to internal auditors, external auditors focus primarily on controls that affect financial reporting. External auditors have a responsibility to report internal control weaknesses (as well as reportable conditions about internal control) to the audit committee of the board of directors.