Internal Controls for Industry - How to Implement and Maintain

(ICI)

KAPLAN

Internal Controls for Industry – How to Implement and Maintain

(ICI)

Mark D. Mishler, MBA, CPA, CMA

KAPLAN

INTERNAL CONTROLS FOR INDUSTRY- HOW TO IMPLEMENT AND MAINTAIN (ICI)

Published in 2021 by Kaplan Financial Education.

Printed in the United States of America.

ISBN: 978-1-0788-1358-7

TABLE OF CONTENTS

Unit 1

Overview

LEARNING OBJECTIVES

After completing this unit, participants will be able to:

- □ Understand and explain the purpose and importance of strong internal controls
- □ Detail the advantages as well as the disadvantages of internal controls for an organization
- □ Explain the difference between controls and processes
- □ Describe management's responsibility to oversee the internal controls of an organization

OVERVIEW

This course's focus is industry internal controls from the perspective of boards of directors, chief financial officers, controllers, and internal audit. As a result, much of course's focus is on the control environment and entity-level controls because of their significant influence on control effectiveness.

The Committee of Sponsoring Organizations (COSO) established the internal control framework which organizations and regulators (the Securities and Exchange Commission, the Public Company Accounting Oversight Board), and standard setters (Financial Accounting Standards Board and American Institute of CPAs) adopted as the basis for internal control over financial reporting (ICFR). COSO principles one through five cover the control environment and entity-level controls.

This course is written for organizations. Much of the published internal control guidance is directed at auditors. This guidance is useful to organizations for aligning their internal controls with auditor processes. This avoids reinventing the wheel by taking advantage of auditor control expertise and knowledge. In addition, it results in a more efficient audit process (lower audit fees) because auditors assess internal controls as a part of their audit.

OBJECTIVE OF FINANCIAL REPORTING

The objective of financial reporting is to provide useful measures and disclosures about an entity's financial performance and financial condition. Users of financial reports employ financial analytical techniques to assess management's performance in creating value historically and to forecast future value. From this financial analysis, users of financial reports make operating, investing, and financing decisions.

The Financial Accounting Standards Board (FASB) formally addressed financial reporting as early as 1978 when it published the first of a series of eight concepts statements. Statements of Financial Accounting Concepts (SFACs) main purpose is to establish the foundation for the FASB's financial accounting and reporting guidance development. SFACs are not codified, and, thus, are not authoritative GAAP.

A secondary purpose of SFACs is to also enable financial statement users to understand the content and limitations of accounting and financial information they use in performing financial analysis. Together with information from other sources, SFACs serve financial information users by facilitating efficient functioning of capital and other markets which promotes efficient allocation of scarce resources based on users' financial analysis.

Underlying this section is the following Statements of Financial Accounting Concepts as they apply to users of financial reporting.

INTERNAL CONTROL SYSTEM - ADVANTAGES AND DISADVANTAGES

The revised COSO Framework, the Public Company Accounting Oversight Board (PCAOB), and the AICPA define internal controls as:

> "a process, effected by the 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"

As we will see soon, the three last words defines the top side of the COSO cube.

"Internal control" was first defined in 1948 by the American Institute of Accountants, but internal control practices have existed since ancient times. According to "Changing Audit Objectives and Techniques" by R. Gene Brown in 1962, ancient Egypt implemented a dual system of internal controls for collecting taxes. In ancient Egypt, one branch of government collected the taxes and a separate branch provided oversight. Since 1977, all U.S. publicly-traded companies have been legally required to follow a defined and enforced set of internal controls.

Internal controls benefit businesses (the author uses the term "business" broadly to include any entity or organization) in two broad areas of (i) financial reporting and (ii) operating efficiency. Too many people, including business management, unfortunately view internal controls as primarily an accounting responsibility for financial accounting and reporting compliance. The larger benefit of internal controls, however, is to ensure a business operates more efficiently.

EXAMPLE

Internal controls over financial reporting and operations are highly interrelated.

For example:

Failures in operating controls can create increased allowances for sales returns, higher warranty expenses, or higher allowances for doubtful accounts receivable.

Failures in regulatory controls can result in regulatory fines, reputational risk/reputational damage, and higher liabilities for workers' compensation expenses or for environmental expenses.

Internal controls are specific restrictions or policies & procedures that guide employee activities to reduce the chances of fraud, significant errors, or unforeseen detriments to a business. Using controls lets company management identify problems earlier before they get bigger and can prevent employees from stealing company assets or resources. Written internal controls help employees understand how to perform their duties, which helps protect the company.

Internal controls are implemented so an organization's activities, policies, and plans are efficiently integrated together to optimize achieving business goals. Internal controls are processes and procedures that direct, measure, and monitor a company's resources to achieve operating and financial goals as well as comply with appropriate regulations.

From an accounting and financial reporting perspective, accounting data are compiled, processed, and evaluated to provide operating feedback and present financial statements to the company's board of directors, shareholders, and regulators.

This control integration is an important point because many companies view internal controls as an ancillary or "add-on" activity adjacent to the company operations. Internal controls have minimal value if not integrated into the company operations.

The assurance threshold for internal controls is **"reasonable assurance"** (see definitions of this term in PCAOB Audit Standards AS 2810.32 and AS 1101.03, and in the COSO 2013 and COSO ERM 2017 frameworks). No matter how well designed or securely implemented, an internal control structure does not provide absolute assurance that a company will achieve its goals or make 100% accurate financial reporting. Nevertheless, reasonable assurance is considered a high threshold.

People design, implement, and operate internal controls. Internal control effectiveness depends on the people following the internal controls. Internal controls apply to all levels of a company hierarchy from the board of directors to the hourly employees performing control tasks. In addition, employee competencies and training impact their ability to properly implement and comply with internal controls. As we will cover later, the control environment adds an additional dimension to control effectiveness.

While the use of internal controls has a number of obvious advantages for a company or organization, there are also disadvantages.

Internal control system advantages to companies are:

- Safeguarding client's assets against misappropriation and misuse, such as being used for purposes that will not benefit the company. Operationally, internal controls facilitate optimal use of company assets.

- Minimizes opportunity for errors and fraud.

An example of an internal control aimed at reducing fraud is requiring employees to submit receipts to receive expense reimbursements within a specified time following travel. Furthermore, a travel policy establishes rules for spending, such as dollar limits of a meal per diem, lodging, entertainment, tips, parking, and taxis. Many companies base these limits on U.S. Government published amounts.

Other examples are requiring two signatures on checks and separating duties that a person who writes a check cannot sign it. Banks often request that businesses submit the signatures of employees who are authorized to sign checks so the bank can verify checks before paying them.

Internal controls can identify potential errors before they occur. No matter how hard one tries, it is not possible to prevent or detect every potential error. In other words, mistakes will happen.

For scenarios relating to detection of errors, rechecking numbers, such as a monthly bank reconciliation, may identify errors that occurred once. In other situations, such as reviewing new contracts a second time after 30 days, may identify ongoing problems. In both cases, internal controls can identify the error.

EXAMPLE

The payroll process requires two people review each payroll before cutting checks and distributing them to employees. Each person independently totals employee hours, calculates their earned pay, and verifies headcount. The two sign the payroll calculation and compare their calculations.

EXAMPLE

A production facility performs a limited test-run on a customer order by checking production quality of the first items produced before producing the complete order.

EXAMPLE

A restaurant uses checklists for opening and closing tasks that employees must perform to ensure health requirements compliance and adequate food inventory levels are maintained.

- Enhances business performance by defining business objectives, asset requirements, and capital needs.

- Communicates financial and operational performance so that corrective actions may be developed and implemented in a timely manner to achieve desired results.

- Provides feedback that can help detect abnormalities.
- Provides monitoring that can increase operating and support function efficiency.
- Supports management's policy implementation to achieve company goals.
- Provides assurance that all transactions are processed completely and accurately; and provides confidence that only authorized transactions are processed.
- Increases financial statement accuracy and reliability.
- Provides assurance that the company's assets and liabilities exist and are correctly stated.
- Facilitates accurate record keeping and provides assurance that adequate documentation supporting transactions is created and maintained.
- Provides accurate date for management decisions in evaluating business performance, developing business plans, and in making resource allocation decisions.
- Helps raise capital by providing financial and operating information to lenders and equity investors.
- Can provide employee motivation which can result in increased performance and profitability.
- Applies some moral pressure on employees.
- Coordinates operations and support functions by defining department and individual roles, responsibilities, and duties. This can boost performance in conducting operations, delegating tasks, and executing efficiently.
- Reduces lawsuits and insurance claims. A company policies and procedures manual with associated controls that lays out staff behavior restrictions can reduce lawsuit risk or costly insurance claims. For example, company policies that address state and federal workplace rules and regulations, such as those covering harassment and overtime, provide guidance for proper behavior. Controls that address workplace safety can reduce accidents, which in turn will lower insurance premiums, workers' compensation claims, and negligence lawsuits.
- Lower external audit costs by resulting in less audit work and fewer audit staff. Specific examples are:
    - reduce the amount of audit work because the auditor can use system-based audit tools
    - enable the auditor to gain greater knowledge of the business and economic environment in which it operates
    - reduce substantive testing with greater use of tests of controls

- reduce testing sample sizes
- minimize chances of errors and fraud
- identify areas prone to errors and frauds, which enables audit planning by allocating more time and effort to those areas
- reduce the amount of audit evidence to be gathered
- strengthens the credibility of audit evidence gathered
- boost company accountability through segregation of duties and identify management contacts for auditor inquiry
- minimize the time required to produce assessments, reports, or opinions
- provide competitive advantage for securing new business
- with a controls certification, enhance reputation in the marketplace in comparison to firms that do not have a controls certification credential

Disadvantages of internal controls are:

- Can be expensive to install and maintain. For example, the physical security systems require qualified personnel to operate them and continuous maintenance and servicing.
- Can lead to over reliance. This may lead to relaxed management supervision and allow account manipulation and asset use. In addition, it may cause a company's auditors to relax other measures of testing for fraud and errors.
- Requires constancy and consistency. An internal control system that is too rigidly designed to allow for organization adaptation may be ineffective or difficult to sustain.
- If poorly designed or implemented, may lead to employee frustration or apathy. Also in this situation, it may expose the company to more errors and fraud.
- Rigid implementation may lead to inefficiencies or a slowdown in business operations.
- Requires continuous updating as the organization changes. If not, the controls may become increasingly ineffective.

Related to disadvantages, weaknesses to internal controls are:

- The people who design or implement an internal control may make mistakes that can lead to that control being ineffective.
- Management may override an internal control.

- Two or more individuals may collude to circumvent what otherwise would be an effective control.

- As processes evolve, the control may become out of date.

Designing effective internal controls requires carefully examining the company's organizational structure. Management needs to identify not only appropriate checks and balances, but identify the employees responsible for ensuring that the controls are implemented and effective. Strong internal controls can keep a company sustainable by helping to achieve four key business objectives:

1. Safeguarding assets. Proper controls protect a business' physical and financial assets from fraud, theft, and errors by preventing or timely identifying errors and fraud that may occur. One of the most essential concepts related to internal controls (and specifically to safeguarding assets) is the segregation of duties (i.e., separating incompatible functions) because it prevents a single individual from requesting, authorizing, verifying, and/or recording business expenditures.

2. Ensuring reliable financial reporting. Management and stakeholders require accurate financial information to make informed operating and investment decisions. Because solid internal controls help to maintain the validity of financial data, they also equip management to make better decisions.

   Controls over financial processes generally fulfill these criteria:

   - Completeness. All records and transactions are included.

   - Accuracy. The correct amounts and other relevant data are recorded.

   - Validity. The transactions captured or recorded were real and appropriate.

   - Authorization. The proper authorization levels are in place to cover such things as approvals, payments, data entry, and computer access.

   - Timeliness. Financial reports are available in a timely manner for decision usefulness.

3. Maintaining compliance. Credible financial data enables companies to achieve compliance requirements to file complete and accurate reports (such as tax returns) and to meet financial reporting obligations (such as loan covenant compliance, shareholder reporting, and SEC financial reporting). Appropriate processes and procedures also allow organizations to meet other regulatory and statutory filing or financial reporting requirements.

4. Accomplishing operational efficiency. Companies operate more effectively with processes and procedures both implemented and followed. A strong internal control environment increases operational and support efficiency through automation of manual controls, removing unnecessary or duplicative process steps, or combining certain functions cost-effectively. Finally, when financial data are consistent and easily accessible, management receives timely and relevant information to verify that business performance activities are in-line with business objectives.

Controls Versus Processes

There is often a misunderstanding of controls and processes.

Controls – are the subject of COSO guidance and SEC and SOX requirements for both companies and auditors to document controls over financial reporting. These requirements include documenting, assessing, and testing controls.

Processes – are the performed activities that underlie controls and can include step-by-step instructions to carry out a policy.

EXAMPLE

	Process	Control
1	Wiring of cash payment to a vendor	Reviewing documentation supporting that wire payment by someone other than the person performing the wire transfer
2	Releasing a customer order for shipment	Confirming that a customer's allowed credit is below the maximum amount allowed in accounts receivable before shipping an order

In "Changing Audit Objectives and Techniques" (1962), R. Gene Brown provides the following table as to evolution of (the concept of) internal control.

Period	Stated Audit Objectives	Extent of Verification	Importance of Internal Controls
Ancient – 1500	Fraud detection	Detailed	Not recognized
1500 – 1850	Fraud detection	Detailed	Not recognized
1850 – 1905	Fraud detection & clerical error detection	Some testing	Primarily detailed Not recognized
1905 – 1933	Fairness determination of reported financial position Fraud detection Error detection	Detailed Testing slight recognition	Increased awareness
1933 – 1940	Fairness determination of reported financial position Fraud detection	Detailed Testing	Interest awakening
1940 – 1960	Fairness determination of reported financial position	Detailed Testing	Substantial emphasis

A study of the table of internal control's historic evolution reveals that internal control practices were rather carried out to detect frauds and that these practices were maintained by 1850s. From 1850s until 1900, it is noted that effort was made to detect clerical errors.

Internal control regulations in the United States arose from needs that emerged following a number of key financial reporting misbehaviors. The most recognized example is the 2002 Sarbanes Oxley Act (SOX), enacted following financial reporting frauds, such as from Enron and WorldCom. SOX is mandatory for all publicly-traded companies in the United States and was a response to such financial reporting issues and had key global consequences. In the similar vein, the COSO (the Committee of Sponsoring Organizations) model, which is the most generally-accepted internal control model today, is deemed the basis model for all internal control regulations and standards across the world today, particularly in EU countries and including international organizations, although it was originally developed in US to prevent development of misleading financial statements.

A key aspect of an internal control structure is that it is an **activity of company management**, rather than that of the finance staff tasked with control duties. Since 1920s, the internal control structure has been closely related to audit work performed by independent auditors. A well-functioning internal control structure can both reduce the independent auditors' financial statement reporting audit testing and shorten the audit time. Audit testing all documents and transactions is maximum audit work and increases the audit cost, especially for companies performing high-volume transactions. A well-designed and effectively-implemented internal control structure relieves the independent auditor from performing detailed transaction testing and, instead, perform tests of controls which saves costs and time.

In 1948 the American Institute of Accountants (AIA) issued the Special Report in Internal Control, which provided the first official internal control definition, Summarized below the definition applies to internal control still today:

> Internal control includes all measures accepted and implemented to protect the organizational plan and assets, ensure accounting information accuracy and reliability, improve operating efficiency, and compliance with corporate management policies.

In 1958, the American Institute of CPAs (AICPA), renamed from the American Institute of Accountants, said internal controls should be divided into two:

1. **Accounting controls** - cover all transactions, methods, and operations directly related to the organizational plan, asset protection, and accounting information reliability. Accounting control examples are control measures for transaction authorization and approval, registration, financial statement development, asset protection, which should be explicitly separated from physical controls over assets and internal auditing duties. With separation of duties and accounting controls, it is highly critical to separate the duties of take-over, protection, and registration of assets and to have different people perform these activities.

2. **Managerial controls** - cover all methods and transactions which are directly related to business operations effectiveness and management policies adherence, but indirectly related to financial records. Managerial control examples are statistical

analyses, time and motion studies, annual reports, staff training programs, and quality control.

International Standards on Auditing (ISA 315) defines internal control as follows: Internal control is a process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations (ISA 315).

Purposes of internal control structure:

- Protect business assets against all kinds of negative situations
- Ensure accuracy and reliability of any business-related information
- Ensure adherence of business operations to determine business policies, management plans, and the legislation
- Ensure economic, effective and efficient use of business resources
- Carry out obligations arising from accountability
- Continuously produce fiscal and management information, and disclose them full-time through regular reporting
- Ensure managerial control
- Ensure accounting control

Purposes of the internal control structure of businesses are summarized as follows (Homes and Overmyer, 1975);

- Protect assets
- Protect against improper spending
- Protect against improper funding and borrowing
- Ensure reliability and accuracy of business and financial operations
- Ensure effectiveness of the business
- Ensure and measure adherence to established policies of the business.

Internal controls apply both to management and finance.

> Managerial controls cover the relationships and contacts established by sales staff of a business in the name of that business, the orders they receive, the returns, and the reasons thereof.

> Financial controls cover the activities by the staff who will make payment or collection, and those who register money transactions into the accounting environment. Internal managerial controls and internal financial controls may often overlap.

These two internal control activities may not be separated by strict lines. All internal controls include all duties. However, business managements take internal financial controls into a deeper consideration. A complete internal financial control is achieved by assessing accuracy of the management's financial transactions and financial entries (registration into the accounting environment and compilation into financial statements). Internal auditors are more interested in internal financial controls than internal managerial controls.

Effective and efficient implementation of the internal financial control structure depends on the following requirements.

- Establish areas of responsibility
- Good planning and good implementation of financial and accounting records
- Effective separation of duties of the business' staff. A good separation of duties will separate the financial roles and responsibilities of an employee from those of other employees. This way, each employee will work independently and hesitation in operations is eliminated, making it easier to perform work. In terms of separation of duties, operations will be planned so as to ensure that no single employee has complete control over all stages of a work or operation. For instance; no single employee may have control over the whole of collections, payments, payrolls, expenses or sales operations. Performance of the work or operation by different people contributes significantly to avoidance of errors and frauds. Similarly, performance of accounting operations by people other than those performing the above will make accounting information, and accordingly financial statements, more reliable to users of this information.

Therefore, internal control is a function of business administration. As businesses grow physically, as their operations grow, diversify, and become more sophisticated and as the types of transactions increase, so do the management's need for reliable information to protect assets, eliminate error, calculate income and assess established business policies and practices. All these needs may only be satisfied by establishment of an effective internal control structure.

Principles of Internal Financial Control Structure

Internal control structure may vary across businesses. An effective internal financial control structure may only be developed by assigning and implementing roles and responsibilities. Key principles of an effective internal control structure as follows (Holmes and Overmyer, 1975):

- Responsibility should be determined for each role. Quality of the control decreases in case of improper assignment or non-determination of responsibility. For instance; if responsibility for collection affairs is not given to a specific staff, the likelihood of theft or disappearance of money from the cash register will increase.

- Accounting and financial affairs should be separated. If collection and payment activities or sales and collection activities are not separated, the assigned staff may embezzle a part of the collection or payment and make registrations to the accounting environment so as to disguise such embezzlement.

- No employee should have full authorization over all stages of a business operation. Any one may commit error, fraud, negligence, carelessness or mistake. If different employees are involved in specific stages of an operation/process, however, the likelihood that one of these employees will notice the mistake will increase unless they connive deliberately.

- To assure accuracy of accounting affairs and operations, a method should be put in place to assess accuracy. For instance; in businesses where retail method is applied, the total value/amount of daily sales must be compared with documentation/receipts of the goods sold.

- Assigned staff should be selected carefully, and trained with regular re-trainings.

- Employees should be bound with a contract. This serves as a deterrent for those who are psychologically ill-intentioned.

- If possible, schedule of the employees/assigned staff should be rotated. The roles filled by acting employees should not be kept vacant.

- Change of roles from time to time will decrease likelihood of fraud, and ensure commitment to the role.

- For each position, a written instruction should be developed. Dissemination of handbooks for operations and controls will both ensure continuous learning and avoid misunderstanding from a single source.

- Protective benefit of the double-entry method in accounting should not be over-relied on. Double-entry practice may not replace control activities. Incorrect entries are hard to detect if double-entered.

- If possible, control accounts should not be overused. Use of control accounts by different people at different rules will help identify errors/frauds.

- Accounting transactions and entries may use mechanical or electronic hardware. Even in these cases, attention should be paid to potential errors and frauds in accounts. Use of mechanical tools, however, will make internal control more effective as it will accelerate and make efforts easier.

Reasons for Assessment of Internal Control Structure. The independent auditor assesses (reviews) the internal control structure for a number of reasons. These are listed as follows.

- Determine, individually or collectively, and through footnotes and remarks, the level of risk materiality arising from unreconciled financial transaction accounts

- Determine evidence collection techniques to be used in audit work

- Identify level of reliability of the internal control structure, and accordingly determine type, quantity and quality of audit evidence to be collected
- Determine whether or not the internal control structure has been implemented as effectively as planned
- Provide evidence as to accuracy, reliability, verity and adequacy of transactions performed in the business
- Determine level of detail of audit work
- Assist with planning of audit schedule
- Assist with planning of audit effort
- Identify weaknesses of internal controls, and provide the management with suggestions to avoid these.

Protect Business Assets

Businesses are founded for a variety of purposes. While some are founded to be useful for the society through direct service, most are founded for profit through production of goods and services. Though indirectly, these serve the society, too. But the main purpose is to earn profit. Businesses maintain their operations by producing goods and services or through trading. No matter their type, businesses acquire various assets for the purpose of producing goods and services or trading. These assets include;

- Direct cash/monetary assets (money, checks),
- Various receivables (with or without note),
- Tangible assets, such as fixtures, machinery, facilities, vehicles, buildings, land/plot,
- Rights in the form of intangible assets, such as rights, goodwill, brands etc.

To attain their purposes, businesses must first protect these assets against all kinds of risks/negative situations. These assets are always facing unwanted situations or risks. Such risks include:

- Theft
- Breakage
- Rust
- Wastage
- Outdatedness and obsoleteness
- Depreciation
- Earthquake, flood, fire etc.

Tangible assets may be depreciated or eliminated due to a number of factors including theft, rust, outdatedness, depreciation or obsoleteness. Business managements take various measures for the purpose of preventing, eliminating or reducing such asset-related risks. It is the management's responsibility to develop a robust, well-executable and effective internal control system at the business so as to eliminate or reduce all such risks.

The following are the asset-related duties of a management:

- Ensure timely delivery of orders
- Ensure conformity of ordered assets with received assets
- Receipt of assets and protection thereof at relevant places
- Enter purchases into inventory cards immediately, and place the same to relevant unit/shelves
- Communicate relevant information to the accounting immediately after the purchasing transaction (ensuring accounting entry)
- Enter outflows to inventory cards immediately
- Prevent theft
- Assess the latest situation from inventory cards, and control the quality of assets
- Ensure proper and efficient use, j) Perform continuous maintenance to extend economic life
- Ensure efficient use (reducing wastage)
- Prevent outdatedness/obsoleteness
- Ensure immediate disposal to prevent depreciation
- Check latest supply at each entry
- Inform the accounting unit, and ensure agreement of records
- Conduct regular inventory counts to identify any theft, wastage, depreciation or breakdown
- Ensure that ordering, receipt, protection and sales of goods, payments and collections, and accounting entries are carried out absolutely by different people
- Avoid ineffective advertising spending
- Ensure accurate and timely transfer of accounting information into the accounting environment

The structure outlined above is the internal control structure relating to assets; and formation, running and maintenance thereof is one of the key duties of the management. Also, measures such as preventing binding of business capital to unused fixed assets (sales/disposal/non-purchase), abolishing production at a loss, sales of fixed assets with exhausted economic life are also protective of assets, and all of these may be identified by an efficient use of the internal control structure. In particular, internal controls relating to retention and safeguarding of cash assets and precious papers are even more important, as they are more likely to be stolen, relocated or hidden and have higher value. Accordingly:

- Those in charge of protection of cash, and those making payment and collection should be different people.

- High amount of money/cheque should be kept at the cash register, and should be deposited to bank account at every day-end.

- Those signing cheques/notes, making payments and transferring these transactions to the accounting environment should be different people.

- Those making purchasing/sales decision, making collection/payment and recognizing these transactions should be different people.

- Bearer cheques should be issued in high values.

- If employees performing follow-up of receivables also have the power to collect, they should be rotated.

- Signing of high-value checks and notes by business shareholders is a critical internal control measure.

- Any deficiency identified with the internal controls should be immediately reported to the senior manager, and necessary measures should be taken.

Business assets are comprised by the assets owned and listed in the assets list of the business balance sheet. Assets or accounting records of the business may be used for unintended purposes. Any physical asset owned by the business may be eliminated or depreciated due to theft, breakage, rust, natural disaster or unintended use. In particular, high-value and easily-portable assets always run a high risk of theft. In businesses lacking a proper and organized inventory and safeguarding mechanism, reliable tracking of raw and other materials proves quite difficult. To avoid unwanted situations concerning assets, the business management should establish a good internal control structure to continuously monitor practices.

To avoid all kinds of risks in businesses, it is critical to establish and continuously supervise/monitor the internal control unit. In this sense, implementing the principles of separation of duties and authorization may constitute effective control measures. Likewise, regular physical monitoring and counting of the assets at places where they are protected are important in terms of protection of assets.

Ensure Accuracy and Reliability of Information

For those who take decision using business information, timely and accurate receipt of accounting information is highly critical. Otherwise, information which is not taken in a timely fashion or is inaccurate may lead to wrong or incorrect decisions. An example to this is the likelihood of loss arising from the decision to participate in the business / purchase shares without knowing accurate profitability and assets.

Reliability and accuracy of accounting information refers to accurate and timely transfer of accounting information to the accounting environment and inaccessibility thereof by unauthorized people. Accounting information of a business should be protected with priority as they form the personality and essence of a business and represent numerical information as to its operations and essence. Accounting information are highly critical in terms of protecting competitive edge, financial strength, profitability and market possibilities of the business; and it is also highly critical to ensure inaccessibility of such information by unauthorized people except where mandatory (legal etc.).

Accuracy of financial information is important in every stage, including classification, summary, registration and reporting of such information. This information is transferred to the accounting environment in accordance with the generally-accepted accounting principles. The information transferred to the accounting environment is transformed into reporting at period-ends (as financial statements), providing information relating to financial standing and operating results of the business as well as other financial information.

These financial statements are presented to the business management through internal reporting, and to the public and stakeholders through external reporting. Business sheet shows the changes in a business' assets, liabilities and equities over a period, and income statement shows expenses/spending/costs and revenues over a period. Both statements have a number of stakeholders. These include potential shareholders, potential creditors, management, shareholders, employees, professional organizations etc. It is management's duty to provide accurate and timely information to all stakeholders.

Accurate financial statements require accurate information. And it is one of the key duties of the internal control to ensure timeliness and accurateness of information. Accurate and timely information ensured by the internal control also ensures effectiveness and efficiency of business operations. If the internal control provides timely and accurate information, comparisons with the costs assumed will be as much accurate and real. Decreased costs may lead to higher effectiveness and efficiency. This way, incorrect and wrong decisions as well as waste of resources will be avoided. In other words, errors, frauds, and other risks may be pre-emptively prevented/mitigated.

One of the key purposes expected of the internal control is to provide accurate, reliable and timely receipt of information from the business' accounting environment and other sources. Reliability of this information is highly critical for those who will take decisions related to the business.

Formation of an internal control structure at a business and constant supervision and monitoring of its effectiveness/practices are directly relevant to/have direct impact on elimination/mitigation of potential errors, frauds, and other weaknesses. To summarize, the most important tool in preventing risks at businesses is the internal control and effective implementation thereof. The business management is directly responsible for any potential error, fraud, corruption and related losses which may arise in case where the internal control structure and practices do not exist.

Efficient and effective use of business resources through effectively implemented internal controls will improve productivity and eliminate unexpected and unnecessary increase in costs. Effectiveness in operations refers to execution of a business' operations in accordance with determined business policies, targets, plans and the legislation.

The internal control structure has direct impact on improving effectiveness in operations. Also, the responsibility to ensure execution of business operations in accordance with the policies, plans and the legislation rests with business management. Improving efficiency of business operations and ensuring alignment of operations with budgetary and managerial policies may only be achieved by developing and effectively implementing the internal control structure (Aksoy, 2006).

Effective and Efficient Use of Business Resources

Establishment and implementation of an internal control structure at a business will ensure proper use of all business resources, prevent unnecessary increase in costs as well as delay in production-sales, purchasing-entry, sales entry processes, leading to increased effectiveness and efficiency in business operations. It will be easier to perform operations effectively and compare operating results with budgetary and estimated results. This, in turn, will document the level of attainment of goals, i.e. level of effectiveness and efficiency.

Efficient use of resources translates into the amount of consumed resources not exceeding the amount of utility (efficiency) attained. If the goal (purpose) is achieved with accurate, timely and minimal use of resources, this will mean attainment of efficiency. Effectiveness refers to level of attainment of planned goals and purposes. Attaining planned production amount stands an example to effectiveness. Therefore, an acceptable level of deviation from planned and realized goals means attainment of effectiveness (Erdoğan, 2009).

Another method in improving internal control efficiency is to continuously inform employees on importance of internal control. To summarize; attaining goals with proper, timely and minimal use of resources means efficiency, while effectiveness (being economical/prudent) means planned costs turning out to be lower than realized costs (Kepekçi, 2004).

Ensure Attainment of Determined Goals and Purposes Implementation of the internal control structure corresponds to its effectiveness. Attainment of goals by business management means achievement of an effective internal control. If inventories are protected, costs are reduced through effectiveness, and achieved and planned targets are comparable, every person performs their duty, timely access to information under authorization scheme is possible, and timely reporting can be made to the management, then the internal control is considered to achieve its goals. This, in turn, corresponds to achievement of internal control goals. The more capable the internal control structure is to prevent or avoid potential risks, the more effective the business is with their operations.

Mitigating and preventing risks through concentration of internal control measures is important, particularly for high-risk areas. In case of identification of risks (theft, etc.) in collections and pays, for instance, higher concentration should be placed on controls relating to outflows from inventory, collections and transfers to the accounting environment. In case of a higher-than-expected rate of wastage, wastage or deficiency in inventories, places where inventories are protected should be kept in better conditions, outdated or obsolete inventories should be continuously monitored, inflows and outflows should be entered to inventory cards on timely basis, and physical inventory should be taken with sufficiently short intervals.

Also, it is important to monitor whether or not values of assets are protected. As all these practices are attainable through internal control, internal controls will provide management with necessary information to monitor:

- Costs/efficiency of operations
- Quality of inventory at the warehouse
- Quantity and amount of inventory at the warehouse
- Comparison of achieved and planned targets and deviation
- Whether or not the principle of separation of duties is followed
- Reliability and timeliness of information
- Whether or not there is unauthorized access to resources

Conclusion: An effective internal control structure is a crucial element in ensuring efficiency, profitability, and sustainability across businesses. An effective control structure is the key to success desired/aimed for a business. It should be noted that building an internal control structure alone will not prove sufficient for success. Internal control structure should, first of all, include a comprehensive and collaborative approach that involves all levels of employees, including executives first, and then lower levels.

Measures required to ensure effectiveness and efficiency of the system should be taken. Continuous performance of activities, identification of potential risks as well as development of suggested solutions on a timely manner is critical to ensure effectiveness of the system. A well-designed and well-practiced internal control structure will contribute to the business in terms of reliability, compliance with regulations, financial reporting, and efficiency in operational aspects. Ensuring effective design and practice of an internal control system should not only minimize fraud and misconduct across the business, but should also add value in terms of growth and sustainability of the business.

Management's Responsibility

Management is responsible for fraud and error prevention and detection and accomplishes this through the proper design, implementation and maintenance of the entity's internal control structure. "Those charged with governance" are responsible for overseeing the strategic direction of the entity as well as its obligations to others which includes the financial reporting process. For purposes of financial reporting for most entities, those charged with governance includes the board of directors as well as representatives from management. The focal point for communications may be the audit committee but this will not always be the case. For smaller entities, the responsibility may rest only with management.

Due to the amount of assistance auditors of smaller entities have traditionally provided their clients, including implementing accounting pronouncements and preparation of financial statements, **management and sometimes those charged with governance may believe that the auditor is part of the internal control structure**. This is definitely not the case. For auditors, this would violate AICPA Independence Interpretation Rule 101-3, Performance of Nonattest Services.

Management is responsible for the entity's internal control. Since management is responsible for internal controls, they are the ones that should determine the extent of their formalization, along with the extent to which the controls are documented. There are three broad categories of formalization.

- **Management reliance only** – when management relies on internal controls only for running the business, it is not as important to have formal controls and supporting documentation. It is still true, however, that without sending a clear message to management and employees, fraud and error are more likely to result. Therefore, internal controls must be present, even if not formalized so that financial reporting objectives can be met. Less formal controls mean that the controls are understood even though they may not be formally documented.

- **Management assertion** – when management asserts to a third party as to the design and operating effectiveness of internal control, it is more important to be able to provide that documentation. This does not mean that management has to make a formal written assertion to an auditor. An assertion occurs when management states that certain controls are in place. Documentation should take the form of narratives, policies, procedures, flow charts and matrices, depending on the size and the complexity of the entity. Under SOX, a written assertion from management is mandatory.

- **Third party attestation** – when the entity is required to have an audit of internal controls or agreed upon procedures performed on some aspect of internal controls, the need for documentation to support the internal controls structure becomes more critical.

For purposes of a financial statement audit for non-public entities, the above second category primarily applies. The quality of management's documentation has become even more important now that the auditor is required to obtain an understanding of the design of internal control and whether it has been placed in operation. This understanding takes place at the entity level of internal control, as well as the activity level.

SECURITIES AND EXCHANGE COMMISSION – INTERNAL CONTROL OVER FINANCIAL REPORTING FOR SMALLER ISSUERS

On March 12, 2020, the SEC adopted various amendments to the accelerated filer and large accelerated filer definitions. The amendments were adopted in part to “reduce unnecessary burdens and compliance costs for certain smaller issuers while maintaining investor protections.” Smaller reporting companies defined as those with less than $100 million in revenues will no longer have to obtain a separate attestation of their internal control over financial reporting (ICFR) attestation from an outside auditor; however, their principal executive and financial officers will continue to be required to certify that they are responsible for establishing and maintaining ICFR, and have evaluated and reported on the effectiveness of their organization’s disclosures and procedures. Although the adoption of the amendments no longer require organizations to obtain an ICFR attestation from an outside auditor, organizations meeting the definition of a smaller reporting company continue to be subject to a financial statement audit performed by an outside auditor who will be required to consider ICFR in the performance of that audit. The amendments become effective 30 days after publication in the Federal Register and apply to an annual report filing due on or after the effective date.[1]

Although the SEC’s goal is to promote capital formation by reducing compliance costs, capital providers and others have expressed concerns about going soft on internal controls and the potential unfavorable results. The potential unfavorable result of going soft on internal controls applies also to private companies.

EXERCISE – SEGREGATION OF DUTIES

Jenny and Jim own a small service company that repairs computers. Jim has another full-time job and Jenny has a 20-hour-a-week part-time job so they rely on the services of a bookkeeper and one other administrative person. The bookkeeper works in the office on accounting and related tasks and the administrative person assists but primarily takes orders and schedules repairs either in the shop or at a client’s place of business. There are two repair people. The company requires payment at the point of service except for two corporate customers so there is very little billing. Most of the payment for services is on site and customers generally use credit cards although sometimes the repair people will receive a check at the client site. Both cash and checks are used for payment at the repair facility.

The company maintains an inventory of parts that are typically used in repair but other items are ordered to meet repair needs.

Instructions

Using the segregation of duties diagnostic, propose a segregation of duties plan for Jenny and Jim’s repair business. Personnel include:

- Bookkeeper – Assume that the bookkeeper works full time (40 hours)
- Administrative person – Assume that the administrative person spends 30 hours a week on taking orders and scheduling and has 10 hours to spend on other tasks
- Non-accounting personnel such as repair personnel could be trained to perform some of the less technical duties

[1] https://www.sec.gov/news/press-release/2020-58

- There is no governing board
- Owners (Jim and Jenny)

Tasks

- Record sales & receivables
- Write checks
- Sign checks
- Reconcile bank statement
- Record expense transactions
- Approve payroll to send to payroll service provider
- Disburse petty cash
- Authorize purchase orders
- Authorize check requests
- Authorize invoices for payment
- Review bank reconciliations
- Sign important contracts
- Make compensation adjustments
- Receive and open bank statements
- Mail checks
- Complete deposit slips
- Make deposits
- Perform interbank transfers
- Prepare invoices
- Review petty cash
- Approve vendor invoices
- Perform analytical procedures
- Initiate journal entries (including to record payroll)
- Authorize journal entries
- Open mail and log cash
- Periodically count the inventory on hand

Bookkeeper	**Administrative Employee**	**Repair People**	**Owners**

Compensating Controls

Smaller entities can also use compensating controls to help mitigate deficiencies caused by the lack of the ability to segregate duties.

EXAMPLE

A small distribution entity had insufficient personnel to properly segregate duties, resulting in a risk that a sales person could sell goods at little or no charge to customers and record the understated charge in the accounting system. Then they could receive a kickback or simply collect more money and not remit it to the entity. If the owner/manager performed a reconciliation of changes in inventory on hand with sales reported by the sales person, it would become apparent that there was a discrepancy. In addition, the owner/manager could review the price per unit sold to see if it was consistent with the price list and follow-up on significant discounts.

Following are examples of other compensating controls that can help a small entity mitigate its lack of ability to segregate duties:

Compensating Control	**How it Works**
Review of reports of detailed transactions	Management reviews reports of detailed transactions to identify errors or fraud. In the sales example above, the manager would consider the transaction date, customer description, dollar amount, and any offsetting account (i.e. discounts)
Review sample of transactions	Management selects a sample of transactions that are chosen from a system generated report or data query program. Data extraction

	software could also be used to choose transactions. The review would consist of the transaction date, customer description, dollar amount, and any offsetting account (i.e. discounts)
Periodic counts of assets and reconciliation with accounting records	Management would periodically count sections of inventory and compare it with inventory records, investigating differences.
Review budget analysis and cost trends	This may be the least effective of the techniques if small thefts or errors.

The issue becomes, "Is management going to consistently perform the monitoring function?" If the monitoring function is consistently applied, the lack of segregation of duties is less important because the monitoring is a compensating control. If it is not consistently applied, then errors or fraud could remain undetected.

Consistent performance of these techniques will also send a message to employees that management cares about asset accountability and will take action against employees who commit fraud. As it relates to errors, it will send a message to employees that care in performing duties is important.

Management Override

Smaller businesses and not-for-profit organizations may have one strong individual who dominates the entity and has a lot of discretion and provides personal direction to employees. Sometimes this is due to the size of the organization and sometimes due to the fact that they either own the business, or in the case of not-for-profit organizations, have a strong personality and believe that they know what is best for their constituents.

On one hand this can be helpful because that person has significant knowledge of the entity's processes, operations, policies and procedures, contractual obligations and generally has a good handle on the entity's risks. But there is a downside.

With this situation there is a high possibility that management could override controls. Clearly, the best guard against this is a strong committed independent board of directors that will challenge the chief executive on issues of financial accountability and accurate financial reporting. However, in closely-held companies, this is not likely to be the case making the prevention of management override very challenging.

Following are some ways to mitigate problems created by or prevent management override:

- Instill and maintain a corporate culture that focuses on and stresses the need for integrity and ethical values. This can be supported and reinforced through recruiting, compensating and promoting people where the values are reflected in their behavior.

- Implement and maintain an effective audit committee chair. Whistleblowers should have direct access to the audit committee chair or a board member (depending on whether the entity has an audit committee).

- System controls that record metadata when a management override occurs. Reports containing the metadata are reviewed independently by someone other than management.

There are some very inexpensive services that will establish and monitor a hotline for people to call. Fraud studies have shown that if employees believe in the ethics and integrity of the entity, they are more likely to report suspicious behavior and less likely to commit fraud themselves. Of course, to accompany the whistleblower program, is a commitment to follow up on issues and to punish violations, no matter how high the person may rank in the entity. Tips and information collected by whistleblower programs are usually the most effective means to uncover fraud and criminal acts.

Note that the cost of anonymous reporting vehicles such as hotlines have come down over the past several years. Many third-party companies provide hotline solutions and other assistance to entities based on the number of employees and services needed.

- Attract and retain qualified members for the board. The audit committee or equivalent should be comprised of knowledgeable independent individuals who are not reluctant to challenge management on issues that arise. They should meet privately with the external auditor. The board should thoroughly understand the entity and be able to identify activities that would have an impact on financial reporting.

- If the entity is large enough and can afford it, an internal audit function that reports to the audit committee would be an excellent mitigating control.

Smaller entities may want to consider the following:

- Instead of a hotline, a designated board member could field calls or even emails. The purpose of the anonymous reporting vehicle is to send a message to employees that their concerns are important. It gives them an outlet to report any suspicious behavior and helps to overcome the presumption of inappropriate management override if the system is effective.

- Add a financial expert to their boards, if they believe an audit committee is not needed. A financial expert would be important if management does not have the skills to prepare its own financial statements. That person could be called upon to assist. It is important to remember that the smaller the management team, the more difficult it is to overcome the presumption of inappropriate management override, especially if the persons are related. An entity may want to contact the state society of CPAs to determine if there are any willing CPAs to serve on boards. Many states have a **Center for Nonprofits** that will assist not-for-profit organizations in finding board members.

Qualified Accounting Personnel

Sometimes smaller entities have a difficult time attracting and retaining qualified accounting personnel who understand and can implement generally accepted accounting principles, and understand the intricacies of financial reporting and have the ability to draft financial statements and disclosures. In many cases, these entities have relied heavily on their external auditors to provide them with advice and expertise in this area.

External auditors of non-public entities, except those who are required to report under Government Auditing Standards,[2] can still assist management with these functions.

However, this circumstance may result in an AU-C 265 comment. AU-C 265 notes that if the entity lacks controls over the selection and application of accounting principles that are in conformity with GAAP (or a special purpose framework if that is the case) this may be a significant deficiency.[3] This involves the entity having enough expertise in selecting and applying the accounting principles.

Another circumstance that could result in an AU-C 265 comment is the lack of qualified personnel in the accounting and reporting function. This involves being able to properly apply GAAP and prepare financial statements, including footnotes. This essentially means the entity does not have someone who has the skills to prepare the financial statements, including notes. Note: There would be no significant deficiency or material weakness if the company outsources the preparation of financial statements to their auditors, as long as the company has personnel with the skills to review the statements, fully understands them, and take responsibility for them, including whether the disclosures are complete. The auditor would determine if this deficiency would be considered a deficiency in internal control, a significant deficiency or a material weakness. To prevent AU-C 265 comments, it may be advisable for companies to seek this advice from someone other than an external auditor. **No matter who is consulted, entity personnel still need to have enough expertise to make their own decisions based on external advice.**

Banking Controls and Other Outsourcing

Banking controls and the outsourcing of transaction processing to third parties can help to mitigate a lack of segregation of duties.

Monitoring Activities

Monitoring activities can be performed by management or by the board. It is important that they are performed thoroughly and with the knowledge of what to look for. Sometimes people who start small businesses, executive directors of nonprofits and board members may have significant content knowledge related to the entity but know little about accounting processes and internal controls. A well-designed control performed by someone who doesn’t really understand it is not effective.

[2] Under GAS, the auditor is able to draft financial statements, including footnotes, but is not able to implement accounting principles for them. The auditor can always provide advice and give management tools and templates to use.

[3] AU-C 265 does not provide examples of circumstances that are ordinarily considered significant deficiencies. There are examples given which can fall into any of the three categories: deficiency, significant deficiency, or material weakness.

NOTES

Unit

2

The Committee of Sponsoring Organizations (COSO)

LEARNING OBJECTIVES

After completing this unit, participants will be able to:

☐ Understand and apply the COSO integrated framework to their organization as illustrated in the COSO cube

☐ Explain why COSO was formed

☐ Identify common missteps to avoid when evaluating internal controls

THE COMMITTEE OF SPONSORING ORGANIZATIONS (COSO)

In 1985, the Committee of Sponsoring Organizations (COSO) was formed to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative. COSO's purpose was to study the factors that could lead to fraudulent financial reporting. As part of its charge, it also developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

The COSO Internal Control Framework provides guidance for companies to document and assess their internal control structure. Prior to the COSO Framework, no official standards existed for companies to evaluate controls over the risk of filing materially false financial reporting or controls relating to preventing other types of fraud.

The sponsoring organizations are professional associations that are headquartered in the United States:

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executives International (FEI)

- Institute of Internal Auditors (IIA)
- Institute of Management Accountants (IMA)

The COSO's goal is to provide thought leadership dealing with three interrelated subjects:

- Internal control
- Fraud deterrence
- Enterprise risk management (ERM)

There are several significant dates of COSO publications:

- 1992 – COSO released its original internal control framework titled "Internal Control – Integrated Framework" which established the framework for internal control and provided evaluation tools for businesses to employ in evaluating their internal control structure.
- 2003 – COSO released draft titled "Enterprise Risk Management" (ERM) to guide management processes to identify and manage enterprise risk. This release neither supersedes nor amends its 1992 internal control framework. ERM is broader than internal control, and internal control is included within ERM.
- 2006 – COSO released internal control guidance for smaller public companies
- 2009 – COSO released guidance clarifying "monitoring"
- 2013 – COSO released its updated Internal Control Framework that superseded its 1992 and 2006 prior releases effective after December 15, 2014.

Business had changed in many ways since the 1992 COSO Framework. There were two primary drivers necessitating an updated COSO Framework in 2013 – information technology and outsourcing.

Information technology advances resulted in increased use of computerized processing of enterprise and accounting activities within companies. As a result, COSO added significant technology and network guidance.

Companies increasingly outsourced functions, either because they were non-core to the business or to reduce costs by using developing country labor wages. Examples are tax accounting and information technology software usage and data storage in the cloud. Companies cannot abdicate its financial reporting internal control responsibilities for a function just because that function becomes outsourced.

PRACTICE POINT

Many companies have not made major changes to their internal control structure processes, policies, and procedures after initially adopting the 1992 COSO Framework. COSO's updated Internal Control Framework is an ideal opportunity for companies to reassess its current practices and update its internal control structure.

EXAMPLE

The narrative documentation for a specific internal control must describe how the company actually performs that activity. With information technology advances and automating accounting processes into computerized systems, how a company performs an activity will have changed, often significantly.

An example is the three-way match of a purchase order, receiving report, and vendor invoice. One company once performed this accounting process control by manually amassing and stapling the three documents together. Later, that company automated that control within its computer system and the only output was exception reports of unmatched items. That company needs to update its control narrative to reflect the changed control activity.

In the United States, the COSO Internal Control Framework is the only overall controls criteria for companies to assess their effectiveness of internal controls requires public companies to choose an appropriate control criteria when assessing the effectiveness of their internal control structure.

The AICPA publishes authoritative guidance for auditors of non-public entities. Note that in this context non-public refers to auditors of all entities that are not required to follow PCAOB standards. AU-C 315, Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement, introduces the definition of internal control as:

> "A process effected by those charged with governance, management, and other personnel that is designed to provide reasonable assurance about the achievement of the entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives." – AU-C 315

This AICPA definition is consistent with COSO's description of internal control which is contained in the Internal Control – Integrated Framework published by the COSO; except that the new COSO definition omits the word "financial" in the phrase "financial reporting". The revised guidance acknowledges that controls are important for all types of reporting. Although it is identified in the guidance, the AICPA does not require the use of the COSO framework.

Publicly traded entities are subject to the Sarbanes-Oxley Act (Act). As part of the requirements to comply with the Act, management must annually select an internal control framework and then assess and report on the design and operating effectiveness of its internal controls. Virtually all public companies use the COSO framework (1992 and now that it is superseded the 2013 version).

Outside the United States, there are limited other internal control frameworks that are conceptually similar to COSO but have not gained traction outside their home country. Examples are: the Canada Criteria of Control framework (COCO), the United Kingdom Turnbull Report, and JSOX in Japan. COSO is the global standard.

The 2013 updated COSO Framework did not change the original (from 1992) five internal control components. These five components are interrelated and have an influence on each other. A brief summary of the five COSO internal control framework components follows:

- **Control environment** – senior management must set an appropriate tone at the top that positively influences the control consciousness of entity personnel. The control environment is the foundation for all other internal control components and provides discipline and structure.

- **Risk assessment** – the entity must be aware of and deal with the financial reporting risks it faces. It must set objectives, integrated throughout its activities, so that the organization operates in concert. Once these objectives are set, the entity is in a better position to identify the risks to achieving those objectives and to analyze and develop ways to manage them.

- **Control activities** – control policies and procedures must be established and executed to help ensure transactions being processed on a day-to-day basis example: sales and expense transactions) or on a periodic basis (example: accruals and consolidations) result in complete and accurate accounting recognition.

- **Information and communication** – this component surrounds the control activities. An example is the accounting system. Whether manual or automated, the system enables the entity's employees to capture and exchange the information needed to conduct, manage, and control its operations. This component covers both internal (management, governance, and oversight) and external (shareholders, prospective capital funders, or creditors) communications.

- **Monitoring** – is management's responsibility, and the external audit function is excluded from the entity's internal control structure. Management must monitor all entity control processes on a regular basis and properly communicate any issues identified. Ideally, an automated monitoring process exists to identify and communicate control findings. These generally are more-desirable preventative controls. Alternatively, entities can employ independent internal audit procedures to identify internal control issues. These generally are less-desirable detective controls.

COSO Approach – Integrated, Flexible, Adaptable

The 1992 original internal control framework titled "Internal Control – **Integrated** Framework". COSO's position is that internal controls are not only integrated with each other but also integrated into a company's overall business processes. Unfortunately, too many companies treat internal controls as adjacent to the business and as limited to a finance department responsibility. One reason may be that internal controls are a cost and do not produce revenues from product manufacturing or service delivery.

Internal controls have limited value by themselves when not integrated into the overall business. The value in internal controls is by helping the company achieve its objectives through relevant, reliable, and timely information used by management to make strategic and operating decisions and to raise capital by communicating financial performance to stakeholders.

Internal control design and implementation needs to be specific to identified risks particular to an entity. Accordingly, the COSO internal control framework is flexible/adaptable and not rigid/prescribed. This is similar to principles-based versus rules-based bright lines for GAAP. COSO expects that different entities will make different choices about how to identify risks and how to design and implement internal controls. Thus, COSO is not a checklist of listed controls.

It matters not whether a well-known particular control is implemented but instead matters whether risks are properly identified and internal controls are effective in mitigating the risk. Management is expected through exercising judgment to determine the cost and benefit of its internal control structure.

EXAMPLE

Elaborate internal controls over cash receipts would be appropriate for a point-of-sale business operating at a summer carnival. This business model has significant cash shrinkage risk.

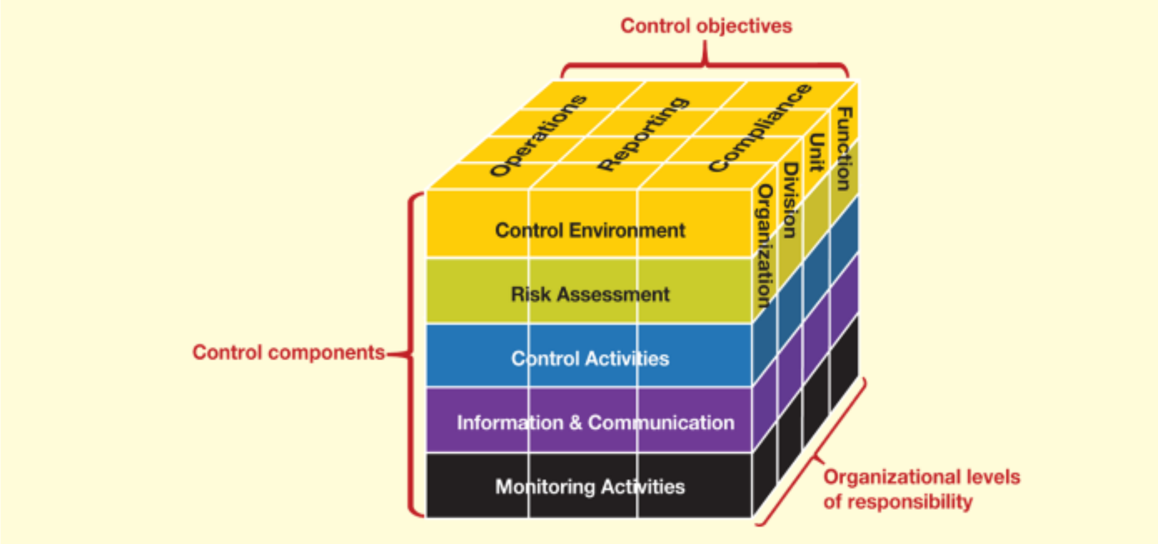
The same internal control structure surrounding cash would not be appropriate for a business-to-business company than receives payment in the form of wire transfers or ACH and never receives cash or checks.

PRACTICE POINT

Many companies improperly implement off-the-shelf internal controls that are too general for the implementing-entity's risk needs. As a result, the internal controls are not effective.

The COSO Cube

EXHIBIT 5.3 Relationship of Control Objectives and Components to Organizational Levels



[4]

Effective Internal Control

The COSO principles are fundamental concepts and so no matter what the entity, the COSO believes that all principles are **suitable and relevant**. Should there be a rare instance where management believes that a principle is not suitable, then it should support this determination. Components and principles should be present and functioning. To determine if this is the case, senior management and the board should determine the level of performance that is necessary given the size and complexity of the entity. This does not mean that the entity will strive for the highest level of performance in applying all of the principles. Rather that management exercises judgment in balancing the cost and benefit when designing internal control.

The framework requires that the components operate in an integrated manner. This means that together they reduce, to an acceptable level, the risk of not achieving an objective. One way to look at this is the controls within the system are a portfolio.

EXAMPLE

- XYZ Fitness Center establishes standards of conduct and sets performance measures and incentives within the control environment to reduce the potential for fraudulent behavior. This impacts the assessed level of fraud risk which is evaluated within the risk assessment component.
- Management develops and deploys policies and procedures as part of its control activities to mitigate the risk identified in the risk assessment process.

[4] From Phillips Libby Libby Ch. 5, 6th Relationship of control objectives and control components

- Management's processing of relevant, quality information within information and communication supports the deployment of business process and transaction controls (**control activities**) and performance of ongoing and separate evaluations within **monitoring activities**.
- Personnel **identify and communicate** control deficiencies to those who would take action to correct them as part of **monitoring activities**. This requires a full understanding of the entity's structures, reporting lines, authority and responsibilities (**control environment**).

The COSO framework (and AU-C 315) identifies five specific components of internal control. They can be best described in two interrelated categories, **entity level controls** and **activity level controls**. As noted in the graphic below, entity level controls encompass the control environment, risk assessment process, information and communication and monitoring. Activity level controls are control activities as well as the portion of the information controls that are related to specific accounting and reporting applications. This includes segregation of duties.

	Entity Level Controls	**Activity Level Controls**
Control environment	✓	
Risk assessment	✓	
Control activities		✓
Information and communication	✓	✓
Monitoring	✓	

It is important to note that just because COSO divided controls into five components, this division does not necessarily reflect how the entity thinks about controls. An original activity of comparing budget to actual or current month results with prior month results is by definition a control activity. However, in some companies where there are few people doing the work, it may also be a monitoring activity. What is important is that the function is performed, not what it is called. At the end of the day, the auditor's primary concern is whether and how a specific control prevents or detects a material misstatement in relevant assertions related to classes of transactions, accounts balances or disclosures. This is one of the reasons why a principles-based framework makes sense and the COSO focuses on the interrelationship of controls.

The entity level controls lay the foundation for the other controls. Without a strong foundation, management and employees are not likely to be as effective in executing the activity level controls. In addition, although strong entity level controls, especially at the control environment, are not an absolute deterrent, they help to reduce the risk of fraud. When management or employees believe that an opportunity is present for fraud, they may be more likely to rationalize a fraudulent act. For this reason, the understanding of the entity level controls should be obtained first. While obtaining information about entity level controls, information will very likely come to light about the interaction between those controls and activity level controls, and then the auditor can determine the further understanding of the activity controls that will be necessary.

The control activities are centered on policies and the procedures that are implemented to execute the policies to ensure that errors and fraud are prevented, detected, and corrected.

Evaluating Internal Controls

Auditors obtain an understanding of internal controls to assess the risks of material misstatement, to plan the audit and design and implement audit procedures tailored to a client's assessed risks. This is true regardless of the size of the entity.

Auditors only obtain an understanding of the control activities considered relevant to the audit. And yet, in a 2019 article written in the Journal of Accountancy it stated that, "in a recent survey of peer reviewers participating in the AICPA Peer Review program indicated that nearly half of the 400 audits they reviewed last year didn't comply with AU-C Section 315, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement, or AU-C Section 330, Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained, because auditors did not properly obtain an understanding of relevant controls."[5]

According to this same July 2019 Journal of Accountancy article by Thorps, Hasty, and Dohrer, the following are the five most common missteps in practice and ways to avoid them.[6]

Misstep No. 1: Assuming the client has no controls

Auditors of less-complex entities often assume that their client has no controls in place. While the controls may not be sophisticated or documented, virtually all clients have some controls over financial reporting.

To identify controls, some questions to ask might be:

- Has management created a culture of honesty and ethical behavior?
- Are login credentials required on computers or operating systems?
- Does the company have policies (formal or less formal) related to the competency of the accountant or bookkeeper?

If the answer to any of these questions is "yes," the client has controls.

Some auditors believe that the only controls they need to consider are control activities, like performing bank reconciliations. AU-C Section 315 explains that internal control is composed of the following:

- The control environment

[5] Thorps, Hasty, Dohrer. "5 Missteps to Avoid When Evaluating Internal Controls." Journal of Accountancy, July 1, 2019. https://www.journalofaccountancy.com/issues/2019/jul/evaluating-internal-control.html

[6] Thorps, Hasty, Dohrer. "5 Missteps to Avoid When Evaluating Internal Controls." Journal of Accountancy, July 1, 2019. https://www.journalofaccountancy.com/issues/2019/jul/evaluating-internal-control.html

- The entity's risk assessment procedures
- Control activities
- Information and communication
- Control monitoring

If a client had no controls in place, there would be no way to prevent or detect and correct a material misstatement. If that's true, it would not be possible to do sufficient audit work to reduce audit risk to an acceptable level.

Misstep No. 2: Not understanding which controls are relevant to the audit

Auditors are required by paragraph .13 of AU-C Section 315 to obtain an understanding of internal control relevant to the audit. This includes all controls assessed as relevant by the auditor and is not limited to those controls that the auditor plans to test for operating effectiveness. Further, control activities relevant to the audit include those control activities that the auditor judges necessary to understand in order to assess the risks of material misstatements at the assertion level.

Controls relevant to a given audit will vary, depending on the client's size, complexity, and nature of operations. Control activities that are always relevant to the audit are defined as those that:

- Address significant risks (including fraud risks)
- The auditor intends to rely upon and test for operating effectiveness
- Address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence
- Support journal entries

Misstep No. 3: Stopping after determining whether controls exist

Peer Review program data show that many auditors think determining whether controls exist is the extent of their responsibilities. Auditors have additional responsibilities of evaluating control design effectiveness and of determining whether the controls are implemented.

EXAMPLE

Evaluating control design over a client's bank reconciliation processes

The procedures involved in the bank reconciliation should be designed to prevent, or detect and correct, a material misstatement.

Does the client's bookkeeper receive the bank statements unopened?

Does the client limit who has access to the online banking account?

If so, the auditor should evaluate these controls to ensure they are designed effectively to address the risks of misstatement.

Directing inquiries at client personnel alone for these purposes is insufficient. The auditor obtains audit evidence about relevant control design and implementation by observing the client applying the controls, inspecting documents and reports, or tracing transactions through the client's financial reporting system. These audit procedures provide evidence that controls are properly designed, implemented, and functioning as intended.

If the control design is ineffective or if the controls have not been implemented properly, the auditor is obligated to evaluate the severity of the deficiency. If a significant deficiency or material weakness is assessed, the auditor is obligated to report these deficiencies under AU-C Section 265, *Communicating Internal Control Related Matters Identified in an Audit.*

Misstep No. 4: Improperly assessing control risk

Peer Review results indicate that some auditors incorrectly believe they can default control risk assessments at the "maximum" level without proper consideration of their client's controls. Auditors should not default to any level of control risk.

Auditors need a reasonable basis for their control risk assessment, regardless of the risk assessment level. Defaulting to a control risk assessment of "maximum" without evaluating the design and implementation of relevant controls could result in failing to identify risks that are relevant to the audit. The control design and implementation evaluation provide the basis for designing a effective procedures to the risk of material misstatement.

The auditor's audit strategy does not require testing the operating effectiveness of controls. Instead, a substantive audit approach may be implemented as long as the audit procedures are responsive and linked to the assessed risks of material misstatement.

Peer Review results also indicate that some auditors incorrectly believe they can lower their control risk assessment without testing whether the controls are operating as designed. If the auditor's response (i.e., substantive procedures) to the assessed risk of material misstatement is based on an expectation that controls are operating effectively, then the auditor is required to perform tests of the controls upon which reliance is placed.

Evaluating control design and implementation is not the same as testing control operating effectiveness. Many auditors confuse the terms "implementation" and "operating effectiveness," but as paragraph .A77 of AU-C Section 315 states, "obtaining audit evidence about the implementation of a manual control at a point in time does not provide audit evidence about the operating effectiveness of the control at other times during the period under audit."

Misstep No. 5: Failing to link further procedures to control-related risks

Once the auditor has assessed the risks of material misstatement including internal control risk, the next step is to design and perform further audit procedures that are responsive to the assessed risks. The auditor should neither automatically perform the same procedures that were required for another client in the same industry nor those audit procedures performed in the prior year.

EXAMPLE

An auditor has two manufacturing clients in the same industry. For both clients, the auditor assessed the risks of material misstatement for the client's rights and obligations assertion in the accounts payable balance as at the maximum level.

Client A's bookkeeper records all invoices in the accounting system once it receives the invoice. Because the invoices are not matched to a purchase order or otherwise reviewed to confirm their validity, the auditor determines that Client A's controls over the recording of accounts payable are ineffectively designed. A specific concern is the risk of recording fictitious invoices.

Alternatively, Client B's bookkeeper records all invoices for authorized purchase orders in the accounting system when it pays the invoice. Because it delays invoice recording until payment occurs, the auditor determines that Client B's controls are ineffectively designed because a risk of unrecorded liabilities exists.

While both clients are manufacturers in the same industry and both have maximum risks of material misstatement related to the accounts payable rights and obligations assertion, both clients may require two very different audit responses.

Client A's auditor may determine that the best way to lower detection risk would be to compare invoices received from vendors with a listing of approved vendors and purchase orders. Conversely, Client B's auditor may lower the threshold amount in performing a search for unrecorded liabilities.

To comply with AU-D sections 315 and 330 when performing audit engagements, auditors should perform all of the following:

- Obtain a robust understanding of the client's system of internal control
- Identify controls relevant to the audit
- Evaluate the design effectiveness of each relevant control and determine whether the controls have been implemented as designed
- Identify and assess the client's risks of material misstatement (including control risk) at the assertion level
- Design and perform audit procedures that are responsive to the assessed risks
- Document the linkage between the assessed risk and the audit procedures.

Following these steps will help drive high-quality, efficient audits that conform to the standards.

NOTES

Unit

3

Steps for Designing and Implementing Internal Controls

LEARNING OBJECTIVES

After completing this unit, participants will be able to:

- □ Understand how management should assess risk in order to properly design effective internal controls
- □ Explain how audit risk is determined and understand how the underlying components used to determine audit risk are affected by the organization's internal controls
- □ Explain how an organization should outsource noncore capabilities and build internal controls around those outsourced services in order to focus its resources on its core competencies

STEPS FOR DESIGNING AND IMPLEMENTING INTERNAL CONTROLS

To design, implement, and integrate internal controls into business operations, management needs to perform four sequential steps:

1. Establish business objectives
2. Identify risks to achieving these business objectives
3. Determine risk management activities
4. Design and implement internal controls when identified as the best approach to manage a risk

The first step is establishing business objectives. The best approach is to begin with a broad scope and then gradually reduce areas as you assess risks at the minimum level for each area. This is consistent with COSO guidance of identifying risks based on business objectives. Financial reporting is a business objective that is germane to this course.

This approach is appropriate for both private companies as well as publicly-traded companies that must formally report on their internal control structure. Because public companies must formally report on their internal control structure, they are a good source of examples and information for private companies. The initial PCAOB guidance in Audit Standard No. 2 (AS No. 2) did not differentiate among risks which resulted in bloated internal controls. Fortunately, Audit Standard No. 5, which superseded AS No. 2, introduced a risk-based approach to internal controls that substantially reduced the number of internal controls. (Audit Standard No. 5 is PCAOB AS 2201.)

EXAMPLE

The author implemented risk-based Audit Standard No. 5. With a risk-based approach, the author reduced the number of internal controls from 268 to 137. This greatly simplified the internal control structure and the work required both internally for compliance and externally for the external audit.

Risk Assessment

As mentioned previously about GAAP and audit standards becoming more principles-based, there are no bright-line rules for assessing business objective risk at the minimum level. Thus, management judgment is paramount in assessing risk. Business objectives with low risk would be out-of-scope for assessing control risk.

Accordingly for public companies, the SEC interpretation is that management's assessment of financial reporting control risk does not need to include every control. Management need only determine whether any financial reporting control material weaknesses existed at year-end which is the date that Sarbanes Oxley requires the CEO and CFO signed representation.

EXAMPLE

In an earlier example, we discussed controls over cash receipts for a point-of-sale business and a B2B company that only receives electronic receipts directly to its bank account. Looking now at revenue recognition for the same two businesses would draw the opposite control conclusion.

The point-of-sale summer carnival business needing elaborate internal controls over cash receipts, would assess revenue recognition risk at a low level and deemphasize revenue recognition controls. This is because the revenue cycle is simple, cut-off is clear, and the customer contract and one performance obligation are straight forward.

The B2B Company on the other hand, which did not need detailed controls over cash receipts, may assess revenue recognition risk at a high level if contracts with customers were complex.

As previously mentioned, there exists no bright-line guidance for management judgment in assessing control risk. Size may be a risk indicator. A common inappropriate approach may be to cover a high portion of total revenue sources for the revenue recognition control risk assessment. This may not be appropriate unless the risks of the different revenue verticals are similar.

EXAMPLE

A company has five revenue streams as follows:

	Annual Revenue	% of total
Product sales	$400,000	67%
Product maintenance contracts	30,000	5
Spare parts sales	100,000	17
Billable engineering	20,000	3
Financing	50,000	8
Total	$600,000	100%

Using revenues, the company can cover 84% of total revenue with two of the five revenue streams. Thus, management may evaluate only those two major revenue streams for the revenue recognition controls assessment. This would be appropriate if the risks for all five revenue streams were similar.

However, if the products maintenance contract and billable engineering revenue streams showed much more variability from year to year and involve more management judgment in determining performance obligations and selling price, then the revenue recognition risks cannot be assessed by only the two major revenue streams.

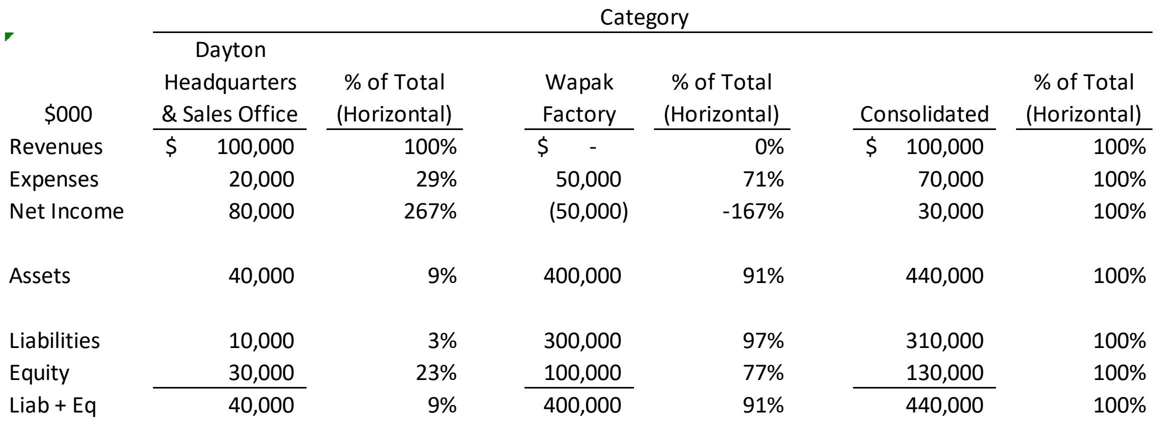
In addition to revenues, other financial areas for conducting the risk assessment process include expenses, income, assets, or liabilities. Management, in performing its initial risk assessment and internal control design process, may analyze the financial statements by disaggregating them into different categories such as geographical location, customer type, product line, etc. The category chosen needs to have a logical relationship to the company's business objectives to support the categorization levels.

Similar to the previous example, after first categorizing the financial statements into categories, the second step is to calculate the relative size of each category relative to the total consolidated financial statement amount. The importance of this process is to identify and assess risk more accurately at the next level down, instead of at the highest consolidated level.

EXAMPLE

This example is simplified for presentation purposes. There may be multiple columns, and if there are significant intercompany transactions, an eliminations column may be necessary.

This company has a headquarters and sales office located near its customer base in Dayton, Ohio and one manufacturing plant located in a lower-cost area an hour away. The columns represent the category level, in this case location because location differentiates this company's business objectives.



	Category					
$000	Dayton Headquarters & Sales Office	% of Total (Horizontal)	Wapak Factory	% of Total (Horizontal)	Consolidated	% of Total (Horizontal)
Revenues	$ 100,000	100%	$ -	0%	$ 100,000	100%
Expenses	20,000	29%	50,000	71%	70,000	100%
Net Income	80,000	267%	(50,000)	-167%	30,000	100%
Assets	40,000	9%	400,000	91%	440,000	100%
Liabilities	10,000	3%	300,000	97%	310,000	100%
Equity	30,000	23%	100,000	77%	130,000	100%
Liab + Eq	40,000	9%	400,000	91%	440,000	100%

Based on this category disaggregation, management can identify business objective risks based on size of financial accounts and business processes.

Revenue recognition, accounts receivable, and intangible asset risks exist at the headquarters/sales office, but not at its manufacturing plant location. Cost of goods sold, inventory, fixed assets, and debt risks exist at the factory location.

For areas excluded from the risk assessment, a good approach is for management to document the risks and implemented controls and the areas to be excluded. In our example above, the product maintenance contracts, billable engineering, and financing revenues combined and individually contribute only a small portion of total revenues. If these three revenue streams share common customers and other economic characteristics with the two major revenue streams, then it may be appropriate to exclude them from management's risk assessment.

The point is that an improper risk assessment could cause potential errors or fraud to become overlooked. Thus, it is important to document evidence and judgment for risks assessed at a low level. Risk assessment is not limited to quantitative analysis as shown in the two previous examples. Even in areas assessed at low-risk, the weakest control areas have historically attracted fraud. This is why guidance also calls for management and external auditors to conduct separately a fraud risk.

Another best practice is a rotating schedule for management oversight over ICFR (internal controls over financial reporting) through internal audits. There is further benefit from adding unpredictability to internal audit scope at each location. This reduces employees' perceived fraud opportunity (part of the fraud triangle discussed separately in this course). Small companies may more-efficiently outsource internal audits to achieve the same goal.

Auditing Standard No. 8 – Audit Risk

PCAOB Release No. 2010-004 covering AS No. 8 – Audit Risk – was effective for public company audits of fiscal years beginning on or after Dec. 15, 2010. Although intended for external audits of public companies, its concepts can also apply to management's risk assessment of ICFR. (AS No. 8 is PCAOB AS1101).

Audit Risk is the risk that an auditor expresses an inappropriate unqualified opinion on financial statements that truly contain a material misstatement. (Audit risk actually applies both ways and to other opinion letter areas.) The audit risk model is:

$$\textit{audit risk} = \textit{inherent risk} \times \textit{control risk} \times \textit{detection risk}$$

The model shows that audit risk is the multiplicative product of the various risks which may be encountered in performing the audit. (In this case, it would be management performing its risk assessment.) To keep the overall audit risk below an acceptable limit, the auditor must assess the risk level for each of the three audit risk components.

1. **Inherent Risk** - the risk arising due to error or omission as a result of factors other than the failure of controls (factors that may cause a misstatement due to absence or lapse of controls are considered separately in the control risk assessment). Basically, effective controls can reduce risk up to a certain point in these areas.

   Inherent risk is generally considered to be higher where a high degree of judgment and estimation is involved or where transactions of the entity are highly complex. Also, activities involving cash carry a high inherent risk.

   For example, the inherent risk in the audit of a newly formed financial institution which has a significant trade and exposure in complex derivative instruments may be considered to be significantly higher as compared to the audit of a well- established manufacturing concern operating in a relatively stable competitive environment.

2. **Control Risk** - the risk of a financial statement material misstatement due to the absence in or failure of the entity's operation of relevant controls.

   Organizations must have adequate internal controls in place to prevent and detect instances of fraud and error. Control risk is considered to be high where the audit entity does not have adequate internal controls to prevent and detect instances of fraud and error in the financial statements.

   Assessment of control risk may be higher for example in case of a small sized entity in which segregation of duties is not well defined and the financial statements are prepared by individuals who do not have the necessary technical knowledge of accounting and finance.

3. **Detection Risk** – the risk that the auditors fail to detect a material misstatement in the financial statements.

   An auditor must apply audit procedures to detect material misstatements in the financial statements whether due to fraud or error. Misapplication or omission of critical audit procedures may result in a material misstatement remaining undetected by the auditor. Some detection risk is always present due to the inherent limitations of the audit such as the use of sampling for the selection of transactions.

   Detection risk can be reduced by auditors by increasing the number of sampled transactions for detailed testing.

Auditors apply AS No. 8 through an audit risk model to manage the macro risk of an audit engagement. Auditors examine the inherent and control risks for an audit

engagement as a part of them gaining an understanding of the entity and its economic environment. As a result, detection risk becomes a residual audit risk after taking into consideration the audit inherent and control risks specific to the entity and the overall audit risk that the auditor is willing to accept. When the auditor's assessment of inherent and control risk is high, the detection risk must become lower to keep audit risk at an acceptable level.

INDUSTRY PRACTICE POINT

The auditor’s audit plan to achieve lower detection risk may be attained by increasing the sample size for audit testing. As a result, audit work and fees increase. This illustrates an additional entity advantage from investing in establishing a stronger internal control structure.

When the auditor’s audit risk assessment is that the inherent and control risks of an engagement are lower, the auditor can set detection risk at an acceptably higher level, which results in less audit work and lower fees.

EXAMPLE

During audit planning of a new client, the auditor identified the following information regarding its client in its audit risk assessment:

- The entity operates in the telecommunications industry, which is highly regulated
- The entity has a large number of subsidiary locations, including foreign operations
- The entity’s CFO comes from a career in the investment banking industry and is not a CPA. In addition, the entity has no internal audit department and its audit committee only includes one member with a background in finance.
- The audit firm's risk policy establishes the maximum audit risk at 10%

The **inherent risk** in the client’s financial statement audit high because the entity operates in a highly-regulated industry and has a complex multi-location subsidiary structure that could more easily misrepresent its financial statements in the absence of stronger financial controls. Additionally, the initial audit is inherently risky because the auditor has a relatively-lower understanding of the entity and its economic and regulatory environment. The auditor assesses the audit inherent risk at a high level of 60%.

The auditor also assesses the client entity’s **control risk** at a high level for two reasons. The client’s accounting and financial reporting activities may not have strong oversight from an audit committee with only one financial expert. The client also lacks an internal audit department which is an important control in a highly-regulated industry. As a result, the auditor also assesses audit control risk at a high level of 60%.

If inherent risk and control risk are each assessed at 60%, at what level must the auditor set detection risk so that the overall audit risk complies with its internal risk management governance?

Audit Risk	=	Inherent Risk	×	Control Risk	×	Detection Risk
10%	=	60%	×	60%	×	Detection Risk

Detection Risk = 27.8%

The audit risk model sets detection risk at 27.8% maintain the overall audit risk below 10%.

Looking at the micro level, fixed assets are generally assessed at a low fraud risk. The nature of fixed assets is large balances, frequent transactions, and their balance gradually declines through depreciation. As a result, fixed assets generally receive minor audit procedures; however, WorldCom is a poster child for management committing financial fraud through fixed assets, among other areas.

EXAMPLE

In the late 1990's, WorldCom was a high-growth company in the low-margin, fixed-cost telecommunications industry due to acquiring over 60 other telecommunication companies from 1995 to 2000. In 1997, WorldCom acquired MCI for $37 billion.

WorldCom then expanded into Internet and data communications, eventually providing 50% of total United States Internet traffic and 50% of total global e-mails. By 2001, WorldCom owned one-third of all data cables in the United States and provided the second-largest volume of long distance phone calls.

In 1999, WorldCom's revenue growth slowed, and its stock price began falling. WorldCom's expenses as a percentage of revenue increased due to the lower revenue growth causing earnings growth to slow. Accordingly, WorldCom's revenues and profit growth became in danger of not meeting Wall Street analysts' expectations.

One fraud was in revenue. WorldCom reduced its acquisition contingent liabilities by $2.8 billion and improperly moved these funds into revenue. That fraud, however, wasn't sufficient to achieve the targeted income that Bernie Ebbers, WorldCom CEO, desired.

Another fraud was in fixed assets. In 2000, WorldCom began classifying operating expenses as long-term capital investments which provided another $3.9 billion in income. These newly classified assets were expenses that WorldCom paid to lease phone network lines from other companies to access their networks. WorldCom also recorded in fixed assets a top-side $0.5 billion journal entry for in computer expenses without supporting documentation.

In 2001, these frauds converted WorldCom's true losses into income of $1.4 billion. A secondary benefit to the frauds is overstating WorldCom's assets.

WorldCom's financial reporting frauds were detected both internally and externally. The SEC became suspicious and made inquiries because WorldCom reported huge profitability while other telecommunications industry participants, such AT&T, were reporting losses.

Epilogue:

Internally from tips received, internal audit uncovered accounting irregularities in acquiree MCI's accounting. Internal audit also uncovered the capital expenditure and undocumented computer expense frauds, as well as other questionable accounting. WorldCom's corporate controller admitted to internal audit that WorldCom wasn't following accounting standards. A month after internal audit began investigating, WorldCom filed for bankruptcy.

In 2004 when it emerged from bankruptcy, WorldCom was renamed MCI. Former CEO Bernie Ebbers and former CFO Scott Sullivan faced fraud and securities law charges. In March 2005, Ebbers was found guilty and sentenced to 25 years in prison. Sullivan pleaded guilty and testified against Ebbers in exchange for a more-lenient five-year sentence.

The initial control design and implementation step requires the most time and effort. Fortunately, there is a steep learning curve that improves efficiency throughout this initial risk-based internal control design and implementation process. Also because business and industries are constantly changing, both business processes and risks may change in future years following initial control adoption. This means that management needs to reevaluate risks and internal controls in future periods.

“Continuous improvement” is one successful approach to maintaining a sound internal control structure in future periods following initial control adoption. Periodically reviewing the risk assessment process and control design is an important control maintenance activity. One method of doing this would be to update the analytical tables in the previous two examples. Continuous improvement creates control process efficiencies and control operating effectiveness.

Companies utilize internal controls for both external reporting and improving operating efficiency. The default thinking about internal controls is generally focused on financial reporting as not to overstate revenues, income, and assets. The operating control may also target not understating revenues, income, and assets. In accomplishing this goal, it is frequently useful for the control basis to be non-financial because the financial control can become inappropriate.

The understating control focuses on improving operating efficiency and also on fraud. Often in performing an internal analysis, the control is based on financial thresholds used to set the frequency and thoroughness of performance monitoring. For example an internal risk-management policy may call for cycling internal audit frequency based on the size of revenues at a location. For example, stores may be audited every three years unless their annual revenues are greater than $10 million, which would require performing internal audit procedures more frequently on an annual cycle due to the higher assessed risk of larger-volume store locations.

A revenues control may not easily detect or prevent internal fraud of an employee syphoning revenues because, if significant, this could keep revenues below the one-year cycle threshold of $10 million. Internal controls would be improved with data analysis procedures that also monitor items such as gross margins, revenues per census level, and freight costs as a percent of revenues, etc.

Risk from Multiple Locations

As discussed above, multiple locations increase inherent risk, and management’s control risk assessment may require different approaches. For example, centralization generally reduces multiple location risk when accompanied with standard centralized policies and procedures enabled by a centralized information technology system. If this centralization is strong enough, management may determine that there is one control for its risk assessment, versus multiple controls determined by the number of locations.

Centralization may not always cover specific location risks either because a cost/benefit analysis makes it impractical to centralize controls required by only a few locations. This may be due to regional differences in the cultural, political, or economic environments. In addition, it can result from the growth pace of either opening new locations or acquiring new locations. There may be a lag time to implement or convert to the standardized central system.

As a result, management needs to consider the risk characteristics and necessary controls for each financial reporting element, rather than making a single judgment for all controls at a location. This can most reliably be accomplished by initially assessing more locations having unique risks (risk is not mitigated by centralization). Later, as evidence is established documenting about locations having lower risk, then remote locations may be included as covered by centralized controls.

Core Competencies and Internal Controls with Outsourcing to Service Organizations

The **core competency** management concept originated in a 1990 Harvard Business Review article titled "The Core Competence of the Corporation" authored by C.K. Prahalad and Gary Hamel. This article introduces a core competency defined by three business activity conditions. First, the activity must provide superior value/benefits to the customer. Secondly, the activity should not be easily replicated by competitors. Thirdly, it should be rare in the industry and among market participants.

Companies develop core competencies through their resources, such as human capital, physical assets, intellectual property, brand equity, and financial capital. These resources combined with the company's capabilities to create core competencies, which consist of how a firm uses its resources to be competitive and operate efficiently.

A core competency is a deep proficiency that enables a company to deliver unique value to customers. It embodies an organization's collective learning, particularly of how to coordinate diverse production skills and integrate multiple technologies efficiently and effectively. A core competency creates a sustainable competitive advantage in the marketplace.

A company's internal investment should be directed toward maintaining its core competencies to ensure they remain unique. Extending this management concept further, companies should outsource or divest noncore capabilities to free up resources to be focused on their core competencies. Outsourcing is essentially a transfer of business to another company whose core competencies include the transferred activities and functions. It is an approach to acquire lower-cost services by specialist providers.

Examples of outsourced services that have been used for decades before the Harvard Business Review article are payroll and defined benefit pension accounting. As technology has evolved, companies began outsourcing its information technology needs to cloud-based information technology and technology network services. Recent trends are outsourcing tax accounting, financial accounting processes, and human resource departments, often to developing countries.

Outsourcing to a service organization presents some complex internal control issues. Many companies falsely conclude that outsourcing relieves them of internal control responsibility because the controls reside outside the reporting entity. Nothing could be further from the truth. If the outsourced activity is important to financial accounting and reporting, then **the reporting entity is still responsible for assessing risk and control operating effectiveness for outsourced services.**

Companies that outsource need to determine whether the outsourced responsibilities need to be extended to include internal controls at the outside entity or whether these controls remain the reporting entity's direct responsibility. In making this determination, reporting entities need to consider the financial statement materiality of the outsourced activities. They also need to evaluate the extent of interaction between themselves and the outsourced organization. In addition, the outsourced activity may include non-financial operating activities. If these activities have high significance to the reporting entity, then there may be additional disclosure requirements, and, in return, disclosure controls.

Unit 4

System and Organization Control (SOC) Reports

LEARNING OBJECTIVES

After completing this unit, participants will be able to:

□ Explain what services organization controls (SOC) reports are and how they are used by organizations and others

□ Describe SOC reports professional requirements

□ Detail SOC reports components

OUTSOURCING

Outsourcing business processes has become very popular for businesses, nonprofits, and governments of all sizes. Outsourcing increased over the past decade due to the 2008 recession, strategic focus on core competencies, pressure to reduce the cost of operations, an increasing virtual workforce, and lack of internal resources or capabilities to perform the functions. Cloud computing has become very popular, and entities that provide those services are a large part of the growth in outsourcing.

According to Deloitte's 2016 Global Outsourcing Survey, there are many reasons why entities outsource administrative and other business processes.

Cost cutting tool	59%
Enables the entity to focus on its core business	57%
Solves capacity issues	47%
Enhances service quality	31%
Manages business environment	17%
Drives transformation change	17%

Also according to Deloitte's survey, the percentage of entities that outsource the following functions are:

Information Technology	72%
Legal	63%
Tax	53%
Human Resources	47%
Finance	42%
Procurement	41%

The COSO framework specifies that controls cover reporting (the 2013 COSO revision expanded financial reporting to include other forms of reporting), compliance, and operations. An entity's management is responsible for establishing and maintaining a system of internal controls no matter where the activities take place. Accordingly, if a reporting-entity (user-entity) outsources an activity, management is required to understand and have assurance that the outsourced provider, referred to as the service organization (SO), has the appropriate internal controls to support its processes.

Larger SOs engage external auditors to test and report on their internal controls because it is much more efficient to have an auditor test the SO's outsourcing processes than to have its user management or their auditors asking questions and requesting access to test the controls themselves. Smaller SOs, such as bookkeeping firms, generally do not hire auditors to report on their process controls. This results in challenges for entities that use these SO's and their user auditors.

SYSTEM AND ORGANIZATION CONTROL (SOC) REPORTS

Evolution of Profession Literature

The AICPA issued SAS 70 in 1992 guiding financial system applications testing. SAS 70 had two sections. The first section was for the SO's auditor to use in understanding and testing controls at the SO. The second section was for user-entity auditors to understand and test the reports of the service auditor to support the user-entity's financial statement audits.

In 2002 congress passed the Sarbanes Oxley Act and created the Public Company Accounting Oversight Board (PCAOB). Shortly thereafter, the PCAOB issued its Statement No. 2 (superseded later by Statement No. 5) which required an audit of a public business entity's internal control over financial reporting. Because these reports were required by public companies to support their systems of internal control, this made SAS 70 reports more accessible and timely for all entities that used SOs.

Because SAS 70 focused on financial statement audits, however, it was not adequate to address nonfinancial aspects of processing. It was the only literature available, so it became sub-optimally used to test these nonfinancial reporting aspects of privacy, security, availability, confidentiality, and processing integrity.

In June 2011, guidance for auditing SOs and testing auditor's reports on SOs changed when the AICPA issued **Statements on Standards for Attestation Engagements (SSAE)** 16, a new attestation standard. SSAE 16 replaced SAS 70 and provided new guidance for understanding, testing, and reporting on SOs (later superseded by SSAE 18). SAS 122 guides the auditor's responsibility to understand and test controls over the SO's processes (AU 402).

In his blog dated June 11, 2012, James Bourke at the AICPA wrote an article for the AICPA[7] describing the reasons for changes in its standards structure. Bourke attributes changes to the rise in the level of cloud computing which provides internet-based SO applications for data processing, storage, and other computing functions. By outsourcing, the user-entity no longer has to deal with software licenses, software updates, and computer hardware costs. User-entity data transmitted over the internet is often personal or confidential; therefore, the user-entity needs to understand the SO's privacy and security controls.

SSAE 16 was replaced by SSAE 18. SSAE 18 provides three different types of reports to address the evolving needs of user-entities.

1. **System and Organization Control (SOC) 1** – SOC 1 reports on the SO's controls over financial reporting. There are two types of reports that a SO can request. A type 1 report focuses on control descriptions and reports on the suitability of control design as of a specified date. A type 2 report adds an opinion on effectiveness to the type 1 report over a specified period. In addition, the user-entity can also read a detail description of the tests that the SO auditor performed and the results of those tests. Neither of these reports are meant for the public and are restricted. They are only meant for the management of the SO, user-entities, and user-auditors.

2. **System and Organization Control (SOC) 2** – SOC 2 reports on the SO's controls over compliance or operations. Examples of aspects tested are security, availability, processing integrity, confidentiality, and privacy. They are tested using predefined trust services criteria. Like a SOC 1 report, SOs can request either a type 1 or a type 2 report, and these reports have the same user restrictions.

3. **System and Organization Control (SOC) 3** – SOC 3, like SOC 2, is based on trust services criteria. The SOC 3 report, however, does not contain a description of the SO auditor's tests of controls, testing results, nor a description of the control system. Thus, it is not as detailed as in a SOC 2 report. The SOC 3 exists for marketing purposes and it comes with a seal that can be used on a SO's website. The AICPA has one logo that is approved for use for service auditors that provide the testing services and another that is used for the SO. The SO must have had a SOC 3 report issued within the past year to display the seal.

Trust services criteria are classified into the following five categories:

- Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

- Availability. Information and systems are available for operation and use to meet the entity's objectives.

- Processing integrity. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

[7] Explaining SOC: Easy as 123, James Bourke
https://www.aicpastore.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2012/CPA/Jun/Easy123.jsp

- Confidentiality. Information designated as confidential is protected to meet the entity's objectives.
- Privacy. Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

The category Security is contained in all SOC 2 reports and encompasses all of the common criteria. Additional category-specific criteria are added for each of the other categories that the SO wishes to add to their report. A discussion of the SOC 2 and SOC 3 criteria and application are beyond the scope of this section.

SOC REPORT PROFESSIONAL REQUIREMENTS

This part focuses on the SOC 1 report because it is the most common report requested by user-entities and their auditors.

Audit guidance for outsourced service organizations exists for auditors in AU 324 for public companies and AU-C Section 402. This guidance is also beneficial for reporting entities for assessing risk and internal controls at the outsourced service organization.

AU-C 402, *Audit Considerations Relating to an Entity Using a Service Organization*, applies to outsourced arrangements where a SO is responsible for processing transactions that ultimately become part of a user-entity's financial statements. It does not apply to services provided where a user-entity specifically authorizes services such as checking account transactions processed by a bank or where a user-entity specifically authorizes transactions that are processed by a securities broker. It also does not apply in instances where an entity holds a financial interest in another entity but no processing is involved.

Management's Need for a SOC Report

Before choosing an SO, management should obtain and evaluate its SOC 1 report. The SOC 1 report is vital to making a good decision on an ongoing basis, and this action is an important control in the vendor selection stage. Management should document its SOC report evaluation, and not view the yearly SOC report as something just only obtained for its auditor.

EXAMPLE

A national health plan commenced operations in a new region of the country. Each region was permitted to make its own decisions on whether or not to outsource its claims processing systems. Initially the volume of transactions was not significant and could be handled internally. However, in 20X2 the entity made an acquisition increasing its subscriber base from 50,000 to 120,000. Management made a decision to outsource claims processing.

The CFO selected a well-known insurance company to perform the service, but did not request a SOC 1 report on the claims processing system. As a result, the CFO did not know if the entity was accurately processing the user-entity's transactions. In addition the CFO was not aware of the missing complementary-user controls that the SO believed needed to be in place at the user-entity to support the outsourced processing as a whole.

At the end of the year, the CFO and Audit Committee were unhappy when the auditors proposed a material adjustment to correct the amount of claims incurred but not reported. If the CFO had obtained the SOC 1 report, the CFO would have noted that the SO auditor identified certain deficiencies in the SO's internal controls. The CFO then would have identified new controls the user-entity should implemented to have complete claims processing controls.

The User-Entity Auditor's SOC Report Use

Key to this assessment is the degree of interaction between the reporting entity and the outsourced services organization. For example:

- High degree of interaction indicates the reporting entity is likely to obtain the information directly to evaluate internal controls by focusing on its own controls over its inputs supplied and the outputs received in return.
  - the reporting entity retains responsibility for authorizing transactions and for maintaining transaction accountability
  - the outsourced activities are limited to recording reporting entity transactions and processing data.
- Outsourced processes, such as payroll processing, have high complexity, which means that testing inputs supplied and outputs received is impractical because testing would require duplicative re-performing of the outsourced work, which would obviate the outsourcing purpose. Thus, the reporting entity would need the outsourced service organization to also provide evidence of its internal control testing and effectiveness assessment. With payroll:
  - the reporting entity can easily test its controls over its inputs provided to the outside service organization.
  - testing the outputs received of payroll tax, withholding, and benefit calculations, however, would require re-performing the work.
- Low degree of interaction means the reporting entity would need the outsourced service organization to also provide evidence of its internal control testing and effectiveness assessment. In this outsourcing arrangement, the outsourced service organization is authorized to initiate and execute transactions without the reporting entity's prior authorization. The reporting entity cannot independently generate a transaction record and, therefore, can only record the outputs received from the outside service organization.

When there is a low degree of interaction between the reporting entity and outsourced service organizations, it is standard practice for the outsourced service organizations to assist their customer/reporting entities understanding the design, implementation, and operating effectiveness of internal controls over transaction processing and outputs received by providing an audit report. This is not altruistic. Without incurring its own internal control audit and providing the audit report to its customer/reporting entities, each customer/reporting entity may inundate the outsourced service provider with questions and may be required to send its own auditors in which would be highly disruptive.

The outsourced services user-entity auditor will follow two steps regarding SOCs. First, determine whether a SOC report is necessary. If so, then second, determine whether the reporting entity obtained the correct SOC report.

Step 1: The Auditor Determines Whether a SOC Report is Necessary

Management is responsible for an entity's internal controls including those over outsourced processes; therefore, it is natural to believe that the auditor will always require a SOC report as audit evidence. This is not, however, always the situation. A user- entity's auditor first should understand the following facts about the user-entity's operations.

- Nature of the services provided by the SO
- Materiality of the transactions processed or financial reporting processes affected by the SO
- Degree of interaction between the SO and the user entity
- Relationship between the user entity and the SO

The interaction between the SO and user entity has significance. In some cases the user entity may be easily able to monitor the activities of the SO. Accordingly, if the auditor was able to understand the design of the controls, determine if they were implemented and test, if needed, at the user entity level, it would not be necessary for the user auditor to obtain a SOC.

EXAMPLE

An auditor was auditing the financial statements of a midsize distribution Company. The Company outsourced its payroll. The Company established controls over the submission of payroll data to the SO, initiating the transaction. The SO executed, processed, and recorded the transactions. In addition, when the Company received the information back from the SO, a manager analytically reviewed it for accuracy and reasonableness. Since the Company had good user controls and the degree of interaction was high, the auditor obtained an understanding of the Company's controls and did not ask for a SOC report. This, however, does not relieve management of the responsibility to understand the SO that they trust with their data.

EXAMPLE

An auditor was auditing the financial statements of a large foundation. The Foundation outsourced its investment management function. The Foundation provided investment parameters to the investment manager who was also the custodian. The SO initiated, executed, processed, and recorded the transactions. When the Foundation received the information back from the SO a manager analytically reviewed it for and reasonableness. However, since employees of the user entity did not initiate the purchases and sales, management did not have a sufficient understanding of what should have occurred, so a SOC report was necessary for the user auditor to understand controls over investments. The SO had the primary accountability unlike the payroll example above. The degree of interaction was too low for the auditor to be able to solely evaluate the user controls. It is important to remember that the Foundation still needs to have user controls in place even when they are not sufficient for the auditor to solely evaluate them.

Step 2: The Auditor Determines Whether the Client Obtained the Correct SOC Report

As noted earlier, there are several types of SOC reports. Neither the client nor the auditor can control which SOC type the SO performs. If the SOC report is unsuitable for the auditor's purposes, additional procedures may become necessary. The following table illustrates different SOC report suitability.

SOC Report	Appropriate When
SOC 1 Type 1	The user auditor simply needs to understand internal controls and does not intend to rely on controls. Control reliance is not necessary if the auditor is able to obtain sufficient evidence to support account balance or class of transactions in other ways.
SOC 1 Type 2	The user auditor needs and element of control reliance. Control reliance is important if the information is solely in electronic form; or if the outsourced service is high risk or very complex.
SOC 2 (Type 1 or Type 2)	A user auditor needs to understand if the SO's information system has integrity in processing, confidentiality is maintained, data are available, privacy is maintained, or data are secure. Typically, this is not the type of assurance a financial statement auditor will need. It may be useful for certain attestation engagements, and, depending on client operations, it may be critical. For example, in an attestation engagement to determine HIPPA criteria compliance, confidentiality would be important.
SOC 3	Not appropriate for user-entity financial statement audits.

EXAMPLE

An auditor was auditing the financial statements of an entity that just began taking debit and credit card payments for online sales. The auditor obtained a SOC report from the client only to discover that it was a SOC 2 report on security. The auditor needed a SOC 1 Type 2 report to have the appropriate level of assurance on internal controls over the financial processing performed by this significant system. The client may have needed a SOC 2 report for their operating purposes, but the user-entity also needed a SOC 1 type 2 report to cover financial transaction processing.

This issue caused the auditor to consider additional audit procedures to obtain the evidence needed. The auditor could:

- Contact the SO through the user entity to obtain information
- Visit the SO and perform procedures
- Use another auditor to perform procedures

- Obtain confirmations of balances and transactions from the service organization
- Perform analytical procedures on information at the user entity's location. (Note that the effectiveness of analytical procedures will vary by assertion as well as by the level of information available.)

A SO does not want additional auditors coming in to perform their own tests. However, in a case where a SOC report is not available, either due to an error, as in the example above, or because the SO has only a few user entities and does not want to pay for a SOC audit. In this event, the user-entity auditor will have to perform additional steps, such as the ones in the example above to get the assurance needed.

SOC REPORT COMPONENTS

This part discusses the SOC 1 Type 2 report components since it is the most comprehensive of the two report types.

Management and the user-entity auditor need to understand the SOC report components. A frequent management mistake is concluding that their work is done if the SOC audit opinion is unmodified. This part identifies what to look for and test in the five SOC report sections, which are listed below:

Section 1: The SO's independent auditor's report

Section 2: Management of Service Organization's assertion

Section 3: Management of Service Organization's description of its system

Section 4: The service auditor's description of tests of controls and test results

Section 5: Other information provided by the Service Organization

Section 1: The SO's Independent Auditor's Report

The independent auditor's report contains important information which should be included in the user-entity's control testing and/or its auditor work paper documentation. Although the guidance language is written for the auditor, this guidance is also appropriate for the user-entity (reporting entity) in documenting its internal control performance and testing.

Understand the Nature of the Service Auditor

The user-entity auditor may or may not be familiar with the SO's auditor. The reason they may not is that not all service auditors are public accounting firms known to possess deep experience in this type of work. Instead, service auditors may be smaller public accounting firms or firms not in public accounting at all. This does not make them inadequate but means the service auditor may not be known by the user-entity auditor.

As a result, the user-entity auditor may make inquiries to be sure that the service auditor is subject to regulatory oversight. For example, the service auditor may be practicing in a jurisdiction with different standards than those set forth in SSAE No. 18 AT-C 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting*.

In addition, the user-entity auditor should assume the service auditor is independent, unless there is evidence to the contrary. Lastly, the user-auditor should apply the guidance in AU-C 620 to document the use of a specialist.

The user-auditor (and user-entity) must determine whether the dates covered by the SOC report and testing performed by the service auditor cover a substantial amount of the period represented by the financial statement audit. This includes evaluating the period elapsed since the end of the SOC report period.

If there is no period overlap, the overlap period is too short, or too much time has elapsed since the end of the period covered by the SOC report, the user-entity auditor (and user-entity) need to determine whether to obtain more evidence. Factors to consider include:

- The significance of assessed risks of material misstatement at the assertion level
- The specific controls tested during the interim period and significant changes to them since they were tested including changes in the information systems, processes, and personnel
- The degree to which audit evidence was obtained about the operating effectiveness of those controls
- The length of the remaining period
- The extent to which the user-entity auditor intends to reduce further substantive procedures based on the reliance on controls
- The user-entity's effectiveness of the control environment and monitoring controls

  When there are period overlap concerns, SO's frequently issue a bridge letter that documents any changes at the SO and bridges the "gap" between the SO's SOC report date and the user-entity's year-end. The letter is written on the SO's letterhead and is typically signed by the SO.

- The bridge letter is a tool used by SOs so that the user-entity does not need to wait for the next SOC report. However, the service auditor does not opine on the bridge period letter; thus, it does not have the weight of a service auditor's report. The bridge letter should address several key points:
  - The report end date
  - Material changes in the internal control environment (if any)
  - A statement that the SO is not aware of any other material changes
  - A reminder that user-entities must follow the complementary user-entity controls
  - A disclaimer that the bridge letter is not a replacement for the actual SOC 1 report

Fortunately, for most SOs, SOC reports are December 31 year ends. Therefore, coverage may not be a big issue. For SOs with different fiscal year ends, the user-entity auditor may have to perform additional procedures.

EXAMPLE

A user-entity auditor obtained a SOC report from management for its payroll application. The application covered a significant number of employees and the majority of the dollars in expenses, so the auditor believed a SOC 1 Type 2 report was needed. The user-entity had good user controls. The SOC report covered the period the period January 1, 20X3 through December 31, 20X3.

The user-entity financial statement period was July 1, 20X3 through June 30, 20X4, meaning the overlap period was six months. Given the quality of the user-entity controls in place, the auditor decided to make inquiries of any changes in systems to the SO. The client facilitated that meeting.

EXAMPLE

An auditor of a medical management company obtained a SOC report from management for one of its claims-processing application. The application covered a significant amount of the dollars that were processed for the user-entity's clients. The user entity's fees to its clients were computed off of the amount of claims processes, so the auditor believed a SOC 1 Type 2 report was needed. The user-entity had good user controls. The SOC report covered the period the period January 1, 20X3 through December 31, 20X3.

The financial statement period was October 1, 20X3 through September 30, 20X4. The overlap period was only three months. With claims processed, however, there is not significant interaction between the user-entity and the SO. The user auditor was concerned that the overlap was not sufficient and requested that the user-entity obtain a bridge letter from the SO which had a practice of creating them. The user-entity auditor, however, ultimately determined that the letter was, by itself, not adequate and performed additional audit procedures.

Identify Important Information in the Service Auditor's SOC Report

The user-auditor will determine whether the opinion on the control suitability (type 1) and control effectiveness (type 2) is unmodified. **The user auditor also needs to be aware of any sub-servicing arrangements.**

SOC Opinion Examples

Type 1 – As noted earlier if a SOC report is a type 1, there will be one opinion in the report on management's description of the system and the suitability of the design of the controls. The elements of a type 1 report follow:

- Management's description of the SO's system
- Based on the criteria in management's assertion, SO management's written assertion about whether
    - management's description of the SO's system fairly presents the SO's system that was designed and implemented as of a specified date

  - the controls related to the control objectives stated in management's description of the SO's system were suitability designed to achieve those control objectives as of the specified date

- A service auditor's report that expresses an opinion on the matters above. Following is the opinion portion excerpted from a SOC 1, Type 1 report.

EXAMPLE

In our opinion, in all material respects, based on the criteria described in ABC Service Organization's assertion the description fairly presents the payroll processing system that was designed and implemented throughout the period January 1, 201X, to December 31, 201X.

the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 201X, to December 31, 201X, and user entities applied the complementary user entity controls assumed in the design of ABC Service Organization's controls throughout the period January 1, 201X, to December 31, 201X.

Type 2 – A SOC report type 2 reports on the suitability of the design as well as whether the controls are effective. The elements of a type 2 report follow:

- Management's description of the SO's system
- Based on the criteria in management's assertion, SO management's written assertion about whether
  - management's description of the SO's system fairly presents the SO's system that was designed and implemented throughout the specified period
  - the controls related to the control objectives stated in management's description of the SO's system were suitability designed throughout the specified period to achieve those control objectives
  - the controls related to the control objectives stated in management's description of the SO's system operated effectively throughout the specified period to achieve those control objectives
- A service auditor's report that
  - expresses an opinion on the matters above
  - includes a description of the service auditor's tests of the controls and the testing results

EXAMPLE

NOTE: Embedded in the report are the following "letters" to highlight key points.

a) coverage period

b) unmodified opinion on the description, the design and the effectiveness of controls

c) discussion of management's responsibility for complementary user controls

Section 1: Independent Service Auditor's Report

To: ABC Service Organization

Scope

We have examined ABC Service Organization's description of its defined contribution recordkeeping system entitled "Description of ABC Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period (a) January 1, 201X, to December 31, 201X, (description) and the suitability of the design and the operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "ABC Service Organization's Assertion" (assertion). The controls and control objectives included in the description are those that management of ABC Service Organization believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the defined contribution recordkeeping system that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in section 5, "Other Information Provided by ABC Service Organization," is presented by management of ABC Service Organization to provide additional information and is not a part of ABC Service Organization's description of its defined contribution recordkeeping system made available to user entities during the period January 1, 201X, to December 31, 201X. Information about ABC Service Organization's business continuity planning and management's response to exceptions identified in the report has not been subjected to the procedures applied in the examination of the description of the defined contribution recordkeeping system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the defined contribution recordkeeping system and, accordingly, we express no opinion on it.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls (c) assumed in the design of ABC Service Organization's controls are suitably designed and operating effectively, along with related controls at the SO. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In section 2, ABC Service Organization has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. ABC Service Organization is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 201X, to December 31, 201X. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a SO's system and the suitability of the design and operating effectiveness of controls involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the SO in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a SO may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a SO may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Opinion (b)

In our opinion, in all material respects, based on the criteria described in ABC Service Organization's assertion

- the description fairly presents the defined contribution recordkeeping system that was designed and implemented throughout the period January 1, 201X, to December 31, 201X.
- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 201X, to December 31, 201X, and user entities applied the complementary user entity controls assumed in the design of ABC Service Organization's controls throughout the period January 1, 201X, to December 31, 201X.
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 201X, to December 31, 201X, (c) if complementary user entity controls assumed in the design of ABC Service Organization's controls operated effectively throughout the period January 1, 201X, to December 31, 201X.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of ABC Service Organization, user entities of ABC Service Organization's defined contribution recordkeeping system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Example Service Auditor's signature

Example Service Auditor's city and state

Date of the Service Auditor's report

Understand the Systems Covered by the Report

SOs frequently provide many different services to clients that span several different SO systems. A particular SOC report may only cover one or two of them.

EXAMPLE

An SO provided payroll and employee benefit services to its clients. The SO had five different payroll systems and three different employee benefit systems. User-entity management must request the appropriate SOC report, and the user-auditor must ensure that the report obtained is for the right system and services.

EXAMPLE

An independent school had a significant endowment fund. A money manager made the investment choices that a custodian processed, and the same financial institution provided both of these services. The financial institution engaged a service-auditor to perform attestation engagements on each of the systems. The independent school's (user-entity) user-auditor was careful to determine that they had the appropriate SOC report for each system because the financial institution had several systems that performed similar services.

The user-auditor noted the SOC report mentioned that one of the tests of controls over the custodial function was over-marking marketable securities to fair value. There were no exceptions to the test performed by the service-auditor. However, the user-auditor noted a sentence relative to alternative investments. It stated that the service-auditor did not test the process for marking those investments to fair value. The user-auditor was curious since the reports produced by the user-entity appeared to have fair values for the alternatives at year end as well as for the marketable securities.

Upon inquiry the user-auditor learned that the user-entity called in those values to the SO. Had the user-auditor not been alert while reading the report he might have continued to believe that the controls over marking investments to fair value applied to the alternative investments as well as the marketable securities since they were both included in the report.

Note if Sub-Servicers Exist

A user-entity might contract with a SO that, in turn itself, outsources some of the services in the agreement to a sub-service organization. These sub-services may be relevant to user-entities' internal control over financial reporting. The sub-service organization may be a separate entity from the service organization, an affiliated company, or other related party. Either way, this could cause the user-auditor to need to consider the controls at the sub-service organization.

Where there are one or more sub-service organizations involved, the interaction between the user-entity activities and the service-entity activities is expanded to include the interaction between the user entity, the SO, and the sub-service organizations. The degree of this interaction, as well as the nature and materiality of the transactions processed by the SO and the sub-service organizations, are significant interest to the user-auditor when considering the significance of the SO's and subservice organization's controls to the user-entity's controls.

The SO may or may not take responsibility for the sub-service organization's controls and may or may not include the description, objectives, and controls in the scope of the service-auditor's engagement. If the sub-service organization is included in the scope, this is considered the inclusive method. If not, it would be considered the carve-out method.

If the services of the sub-servicer are carved out, then the user-auditor must evaluate the effect on the controls over that system as a whole and determine whether internal control deficiencies in the portion(s) carved out could cause a material misstatement. The user-auditor's report will note sub-servicers existence, as will management's assertion.

Following is an example of language that would be included in the report if the services were carved out.

EXAMPLE

Example Service Organization uses Computer Subservice Organization, a subservice organization, to provide hosting services. The description includes only the control objectives and related controls of Example Service Organization and excludes the control objectives and related controls of the subservice organization.

Section 2: Management of Service Organization's Assertion

Management is required to make a written assertion. Until recently it was thought to be required to be a separate part of the SOC report but SSAE No. 18 AT-C 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting clarifies that management's assertion may be

1. attached to management's description of the service organization's system, or

2. included in the description as long as it is clearly separated from the description.

One way to separate management's assertion from the description is through the use of headers. This point is important because the assertion is management's and the service auditor is not reporting on it. More often, management's assertion will be on letterhead. It does not have to be signed by management.

There are three primary clauses that are important in understanding the report.

- The description of the service organization's system must fairly present the system, which was designed and implemented at either a specific date when performing a SOC 1 Type 1 audit, or throughout a specified period of time when performing a SOC 1 Type 2 audit, using AT-C 320 requirements.
- The assertion must state that the control objectives stated in the service organization's system description were suitably designed to achieve those control objectives at either a specific date when performing a SOC 1 Type 1 audit, or over a period of specified time when doing a SOC 1 Type 2 audit.
- The assertion must also discuss the criteria used along with additional statements regarding risk factors that may relate to controls and control objectives for a Type 2 report, ensuring that controls were consistently applied over the specified time frame.

EXAMPLE (SOC 1, TYPE 2 ASSERTION)

December 18, 20X1

We have prepared the description of Example Entity's Dental Claim Processing System entitled "Description of Example Entity's Dental Claims Processing System" for the period October 1, 20X1 to September 30, 20X2 (Description) for processing dental claims transactions throughout the period October 1, 20X 1 to September 30, 20X2 for user entities of the system during some of all of that period and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understating to consider the Description, along with other information including information about controls implemented by subservice organization and user entities of the system themselves, when assessing the risks of material misstatements of the user entities' financial statements.

Example Entity utilizes XYX as a subservice organization to provide certain hosting operations, data center management and network management services to Example Entity's claims processing system. The Description only includes the control objectives and related controls of the subservice organization. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The Description does not extend to controls of the subservice organization.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity control assumed in the design of Example Entity's controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to the controls of the user entities.

We confirm to the best of our knowledge and belief that:

- the Description fairly presents Example Entity's Dental Claim Processing System made available to user entities of the System during some or all of the period October 1, 20X1 to September 30,20X2 for processing their transactions as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

(Criteria not presented due to space constraints)

- the Description includes relevant details of changes to the Systems during the period covered by the Description.
- the Description does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their auditors and may not, therefore, include every aspect of the System that each individual user entity of the Sytsma and its user auditor may consider important in the user entity's own particular environment.
- the controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period October 1,20X1 to September 30, 20X2 to achieve those control objectives, if subservice organizations applied the complementary subservice organization controls and user entities applied the complementary user entity control assumed in the design of Example Entity's controls throughout the period October 1, 20X1 to September 30, 20X2. The criteria we used in making this assertion were that:
  - the risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the services organization
  - the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved, and
  - the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Example Entity
October 18, 20X2

Management's assertion is typically written from the point of view that the service auditor's opinion is unmodified. However, if the service-auditor modified the report, then management's assertion would reflect any modifications.

In addition, if situations exist in which the complementary user-entity controls or complementary sub-service organization controls were necessary to achieve the service organization's control (as reflected in the example assertion above), then management's assertion would be expected to reflect those as well.

The user-auditor is primarily looking for four things in the assertion.

- **The description, in order to ensure that their need for a SOC report on a relevant basis is included in that description.**
- **The period of time covered in the assertion. The user auditor will look for overlaps.**
- **The assertion should be on the suitability of the design of the controls and their effectiveness (if the user auditor needs a type 2 level of assurance),**
- **The assertion has not been modified for an auditor's modification of the opinion.**

Section 3: Management’s Description of the System

Management’s description begins with an overview of the system’s operations and the scope of the report. It then discusses:

- Relevant aspects of the control environment, risk assessment, control activities, information and communication and monitoring
- Transaction processing
- General computer controls
- Control objectives and controls
- Subservice organizations
- Complementary user controls.

Scope of the Report

The user-auditor will confirm that the report is appropriate to meet their needs.

- The standards used to audit the service organization are AU-C 320 (as clarified and re-codified) by SSAE 18
- The portion(s) of the system covered by the report and those related portions that are outside the scope
- Optional services for user-entities that are related but outside the report scope

Often there will be a table of services covered when there is a larger system. As shown in the following example, there are multiple related SOC reports for this entity.

EXAMPLE

Process Name	**Hosting operations, data center management, and Network Management Services SOC 1 Report**	**Comprehensive Payroll Services SOC1 Report**
Logical Security		
■ Application Logical Security		X
■ Application Logical Security	X	X
■ Infrastructure Logical Security	X	
Application Development and Program Change Management		X

Operating System (O/S) and Infrastructure Change Management		X
Physical Security		
■ Housing Locations	X	
■ Transaction Processing Locations		X
Environment Systems	X	
Computer Operations and Data Backup		
■ Data Backup	X	X
■ Data Transmissions	X	X
■ Computer Operations		X
Network Monitoring and Incident Management	X	
New Account Set Up		X
Client data receipt		X
Bank data processing		X
Bank transaction processing		X
Reconciliation and Trust Accounting		X

Relevant Aspects of System Controls

This section provides a detailed description of the entity-level internal controls, control activities, and general computer controls. It is a significant section because it allows management and the user-auditor to evaluate whether the controls on which they would need assurance are included.

If the controls are not sufficient for the user-auditor’s purposes, then the user-auditors may need to identify the gaps and perform additional audit procedures. For example auditors may:

- Inspect records and documents held by the user entity. This may be difficult if the user entity does not maintain adequate detailed records for transactions performed on its behalf.

- Inspect records and documents held by the service organization. The right to inspect records could be a right established between the user entity and the service organization, perhaps as a contract term in the service agreement. If they have not established this right in advance this could prove difficult.

- Obtain confirmations of balances and transactions from the service organization.

- Perform analytical procedures on records maintained by the service organization.

Complementary User-Entity Controls

The SO designs its internal controls assuming that additional controls will be implemented by user entities because it is not feasible for a SO to have certain controls in place that should be performed outside their entities. Therefore, to ensure that the auditor is testing the system in a comprehensive way, the user-auditor should evaluate user-entity controls.

Often, there are numerous user-entity controls identified in a SOC report. The user-entity should evaluate these controls to ensure that the user-entity designed its system of internal controls with these user-entity controls in mind. The user-entity needs to be aware that the SO identified these controls and that there could be other controls that user-entity management believes are important to implement.

The user-auditor should identify the controls they deem to be **key controls** and understand and test those controls. If the user-auditor does not intend to rely on controls, it is still important to understand the controls design and determine that the controls were implemented. Failure of a user-entity to have the appropriate user controls in place is an internal control deficiency.

The complementary user-entity controls may be included in Section 3 along with the SO's internal controls description. Alternatively, the complementary user-entity controls may be included in Section 4 with the service-auditor's description of its internal controls tests and test results.

Following is an example, in part, of a SO's suggested complementary user-entity controls for a retirement plan.

EXAMPLE

Control Objective #1: Controls provide reasonable assurance that new retirement plans are established accurately and completely and are properly authorized. The Plan sponsor/employers/TPAs are responsible for ensuring that:

- Plan changes are approved and provided timely to confirm that setup of the plan is accurate and timely
- Applicable governing agreement or documents are complete and accurate

Control Objective #2: Controls provide reasonable assurance that participant statements are accurate and complete. The Plan sponsor/employers/TPAs are responsible for ensuring that:

- Timely review of account information provided by Example SO of participant is statement along with related activity, is performed by the user, and written notice of discrepancies is provided to Example SO in a timely manner to confirm there is no unexpected activity

Section 4: Service Auditor's Description of Tests of Controls and Test Results

The SO auditor provides descriptions of control objectives, controls, tests of controls, and test results of transactions and entity-level controls. The description of the tests on

the entity-level controls is briefly described as are the procedures that the SO performed for assessing completeness and accuracy of information produced by the SO.

EXAMPLE FROM SOC 1 TYPE 2 REPORT

Tests Performed on Entity Level Internal Controls

In planning the nature, timing and extent of our testing of the controls specified by Example SO, we considered the aspects of Example SO's control environment, risk assessment processes, information and communication, and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Procedures for Assessing Completeness and Accuracy of Information Produced by the Entity

For tests of controls requiring the use of information produced by the SO, procedures were performed to assess the reliability of the information including completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the examination procedures. This includes information produced by the SO and provided to user entities, information used by the SO's management in the performance of controls such as periodic review of user listings and information provided by the SO used in the performance of our examination processes.

If the service auditor uses the work of internal audit, Section 4 will describe the tests performed and the test results.

EXAMPLE

In performing our examination of the Description, the Service Auditor used the work of the SO Internal Audit department to assist in determining whether the controls related to the control objectives stated in the Description were operating with sufficient effectiveness to provide reasonable assurance that those control objectives were achieved throughout the period January 1, 20X1 to December 31, 20X1. Internal audit work was used to provide evidence for the following processes affecting control objectives 3 through 8.

- Control objective #3 - Controls provide reasonable assurance that retirement plan contributions and processed accurately, completely, and timely.
- Control objective #4 - Controls provide reasonable assurance that retirement plan disbursements are processed accurately, completely, and timely and are properly authorized.
- Control objective #5 - Controls provide reasonable assurance that participant accounts are updated and the system appropriately reflects those changes.
- Control objective #6 - Controls provide reasonable assurance that application software development and operating system changes are authorized, tested, and approved prior to production implementation.
- Control objective #7 - Controls provide reasonable assurance that access to production program data files is restricted to authorize users and programs.
- Control objective #8 - Controls provide reasonable assurance that program jobs, including data backups, are processed when scheduled and that processing errors are identified in a timely manner.

The testing nature performed by internal audit relates to controls over routine processes and includes inquiry of relevant parties who perform the control activities, observation of the performance of the control activities at different times during the examination period, inspection of samples of documents evidencing the functioning of controls, and re-performance of certain controls operation. Any deviations identified by Internal Audit are included in the results of testing that follow.

In connection with using the work of Internal Audit, the SO Service Auditor obtained the work papers supporting the tests performed and reviewed the work papers to evaluate whether the work was:

- Performed by a person having the appropriate skill and expertise
- Properly supervised, reviewed and documented
- Supported by sufficient, appropriate evidence to draw reasonable conclusions that were appropriate in the circumstances and consistent with the work performed
- Appropriately resolved when exceptions or unusual matters arose

In addition, the SO Auditor:

- Selected a sample for re-performing testing and selected a subsample of each sample selected and re-performed testing
- Inspected the supporting documentation for all other tests to evaluate the consistency of the work papers to the supporting documentation. No deviations were noted as result of our testing procedures.

Following is an example of a service auditor's testing and testing results of control activities.

EXAMPLE

Control objective #1: Controls provide reasonable assurance that new retirement plans are established accurately and completely and are properly authorized

	Controls specified by SO	**Testing performed by SO Service Auditor**	**Testing Results**
1.1	Applications are logged into the XYZ system. The plan is activated on all the applicable systems after the appropriate information has been received.	For a sample of new retirement plans, determined through inspection that the applications were logged into the XYZ system upon receipt and the plan exists on the applicable systems. For a sample of new retirement plans, determined through inspection that applications were activated into the appropriate system after the contract was approved by the plan sponsor.	No deviations noted
1.2	Licensing and appointment for the sales representative area reviewed before the installation begins.	For a new retirement plan, determined through inspection that the check for licensing and appointment of the sales representative prior to installation was performed.	No deviations noted

1.3	Applications are reviewed for completeness and accuracy by the installation maintenance consultant.	For a sample of new retirement plans, determined through inspection that applications were reviewed for completeness and accuracy and documented in the XYZ system.	No deviations noted
1.4	Perform independent verification of accuracy and completeness of new contract setup for all new contracts by the Quality Team. Document resolutions for any issues identified.	For a sample of new retirement plans, determined through inspection that an independent verification was performed for accuracy and completeness by the Quality Team. If issues were identified, a resolution was documented.	No deviations noted

In the previous example there were no deviations. The user-auditor will ensure that it does not take for granted that, just because an opinion is unmodified, there were no deviations that need to be considered by the user-auditor. It may only be that the deviations were not sufficient to modify the service auditor's opinion. Deviations should be taken seriously and evaluated to ensure that they are not significant enough to alter the user-auditor's conclusions about the overall control effectiveness. Following is an example of a test where a deviation was noted.

EXAMPLE

Control Objective #8: controls provide reasonable assurance that program jobs, including data backups, are processed when scheduled and that processing errors are identified in a timely manner.

	Controls specified by SO	**Testing performed by SO Service Auditor**	**Testing Results**
8.1	Formal procedures exist and are followed for problem management and scheduled jobs. If jobs do not complete successfully, procedures are in place to open a ticket and on-call support people are engaged to resolve the issue. Notifications are sent to the support personnel and management before closure of the ticket within 5 business days.	Inspected problem management and scheduled jobs procedures to determine whether they were current. Inspected a sample of job terminations to determine whether they were identified and resolved. Inspected a sample of operations incidents and determined whether they were documented and resolved.	Deviation noted: For 6 out of 25 samples selected for failed jobs testing, the "Service Now" ticket was not closed in a timely manner. Management's response: Failed scheduled jobs automatically create incident tickets and are forwarded to the operation center staff for follow-up. The process is for ticket within a timely manner. The Server hosting the scheduler was replaced during normal refresh and renamed causing an error in the closure process. The error was found and the server name replaced allowing the process to resume June 17, 20X1. The 6

			incidents identified were reviewed and subsequently had been closed during the testing period during the normal review process.

The user auditor evaluated the deviation and determined that the impact on the internal control structure was not significant based on his understanding of the control objective, the deviations noted and management's response. In this case the auditor determined that there were compensating controls at the SO that detected the issue and it was corrected.

Section 5: Other Information Provided by the Service Organization

Section 5 provides the user-entity with additional information that the SO wants to communicate. For example, the SO might provide information on its bond rating, fidelity bond program, business resiliency program, and environmental safeguards. The SO auditor disclaims an opinion on the other information.

Unit 5

Control Environment

LEARNING OBJECTIVES

After completing this unit, participants will be able to:

☐ Explain the 5 COSO principles under the control environment

☐ Use their new understanding of how the “tone at the top” impacts the control environment to affect change

☐ Describe audit committee leading practices

☐ Improve organizational governance

☐ Use employee code of conduct to effectively impact the control environment

☐ Create an effective whistleblowing environment

The control environment is the board of directors’ and senior management’s overall attitude, awareness, and behavior toward the internal control structure and its role in the organization. It is pivotal to establishing the organization’s ethical standards because of how it influences employees’ control system perceptions. Following are many items that influence the control environment.

- How the board of directors’ and senior management’s actions, speaking, and writing communicates integrity, moral, and ethical values
- Established and communicated ethics policies defining and prohibiting conflicts of interest, such as receiving gifts from third parties
- Established and communicated moral guidance, such as an employee code of conduct and ethical behavior
- Established human capital policies for hiring, promoting, and rewarding employees, such as current position descriptions, training to develop employee skills, and recognizing ethical performance

- Established authority levels, accountability, and an organization structure
- Proper oversight and engagement by the board of directors
- Focus on risk identification and mitigation
- Internal control structure design and implementation, such as for segregation of duties
- Performance evaluation process with corrective actions

Recall the five COSO framework components:

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information & Communications
5. Monitoring Activities

COSO lists the Control Environment component first because it most influences control performance. An ineffective Control Environment will negatively impact the other four components effectiveness. An unethical "tone at the top" or tendency for management overriding internal controls will render ineffective well-designed and implemented controls because of its negative influence on employees control consciousness.

This unit addresses the five COSO principles under the Control Environment:

Principle 1 – Demonstrates commitment to integrity and ethical values

Principle 2 – Exercises oversight responsibility

Principle 3 – Establishes structure, authority, and responsibility

Principle 4 – Demonstrates commitment to competence

Principle 5 – Enforces accountability

This section finishes with "tone at the top" and an organization code of conduct.

Entity-level controls establish the foundation for **activity-level controls**. Non-financial management often think of internal controls in terms of controls at the transaction or activity level such as segregation of duties, performance of bank reconciliations, authorization of transactions, and analytical procedures on account balances.

Entity-level controls caused infamous corporate failures such as Enron, WorldCom, the Baptist Foundation of Arizona and others. One study by the International Federation of

Accountants and the CIMA in 2004 noted that the main reasons for corporate failures were:

- Failure in communicating the tone at the top
- Ethics issues on the part of management
- A weak board of directors
- Lack of an internal control, compliance and/or risk management function
- Aggressive earnings management

Therefore, it is just as important to have a strong foundation (corporate culture) at the entity level to reinforce the individual control activities. With the appropriate tone at the top and monitoring controls, employees are less likely to believe that they can "get away with inappropriate behavior". Thus, entity level controls can serve as a deterrent to fraud, and minimize conflicts of interest.

Principle 1 – The Organization Demonstrates Commitment to Integrity and Ethical Values – Actions Speak Louder than Words

COSO identifies that management **actions** demonstrating integrity and ethical values have a significantly greater impact on the Control Environment than a written document or oral representations. Thus, management actions establishes a ceiling on internal control effectiveness. Integrity and ethical values impact control design, implementation, operation, and testing results.

Integrity is defined as: the quality of consistently being honest, truthful, and having strong moral principles that one refuses to change. Consistency is behaving the same way regardless of the situation. Someone that intentionally reflects on their behavior, communication, and decision-making in a way that reflects their morals and values.

The Institute of Management Accountant (IMA) Statement of Ethical Professional Practice is an ethical guide for management accountants. One of the IMA standards is integrity, which the IMA defines as follows:

- Mitigate actual conflicts of interest. Regularly communicate with business associates to avoid apparent conflicts of interest. Advise all parties of any potential conflicts of interest.
- Refrain from engaging in any conduct that would prejudice carrying out duties ethically.
- Abstain from engaging in or supporting any activity that might discredit the profession.
- Contribute to a positive ethical culture and place integrity of the profession above personal interests.

A leader exhibits integrity by making rational decisions regardless of their mood or current situation, which is an example of consistency of actions and outcomes. Honesty is a refusal to lie, steal, or deceive in any way. This course discusses ethics in a separate section.

Management demonstrates integrity and ethics by taking action several ways. First, individual leaders must possess high morality, ethics, and honesty which establishes company behavioral standards.

Second, management and individual leaders develop and communicate company behavioral standards to its employees throughout the organization. These behavioral standards may exist in several documents, such as a mission statement, ethics policy, employee code of conduct, equal opportunity employment policy, and sexual harassment policy.

In smaller organizations, this communication is generally informal because senior leadership interacts with all employees frequently. In larger organizations, however, this communication becomes more formalized, such as with published statements about how to behave conduct business internally and externally. Unfortunately this communication approach in larger organizations is often stale or occurs infrequently, such as annually or only on an employee's first day of work when the new employee is given written behavioral standards that gets lost as a part of a multitude of other paperwork.

As a result, the third way management demonstrates integrity is frequent and consistent reinforcement, such as through company publications and employee training. Without reinforcement, the behavioral standards lose their influence.

The mere existence of company behavioral standards is an insufficient control. Reinforcement measures to monitor compliance about whether employees have read (and hopefully understand) these behavior standards is important. The measures could range from employees annually signing the statements (relatively weak) to on-line videos with follow-up questions for the employee to answer with a minimum number of correct answers required to pass.

Furthermore, company behavioral standards involve management in more ways than employees. Not only should management have the same control compliance monitoring and training exposure as employees, but also regular policy review controls need to be present. Regular review of behavior standards both keeps the standards within legal and regulatory compliance and also keeps the standards fresh, current, and relevant.

Visible management actions, in smaller companies, or press reporting about company actions in larger companies demonstrate to employees that "actions speak louder than words." Particularly influential is how management deals with problems, especially when there are high costs for identifying, preventing, and resolving problems.

EXAMPLE

In October of 1982, Johnson & Johnson maker of Tylenol the leading pain-killer medicine in the United States with 37% market share, faced a tremendous crisis when seven people in Chicago died after taking extra-strength Tylenol capsules. An investigation showed an unknown suspect tampered with product already on the drugstore shelf by adding deadly cyanide into Tylenol capsules.

The tampering occurred once the product reached the shelves. The unknown suspect removed Tylenol bottles from drugstore shelves, infected capsules with cyanide, and then returned the poisoned bottles to the drugstore shelves. Immediately after the publicized cyanide poisonings, Johnson & Johnson's Tylenol market share dropped from 37% to 7%.

Johnson & Johnson faced an ethical and moral dilemma of the best way to deal with the problem. Although management knew Johnson & Johnson was not responsible for the product tampering, management assumed responsibility by ensuring public safety first and recalling all of their capsules from the entire country. This amounted to 31 million bottles and a loss of more than $100 million.

Tylenol reacted very quickly and in a positive manner because of the company's mission statement, initially written in the mid-1940's by CEO Robert Wood Johnson. The mission statement said the company's responsibilities were to the consumers and medical professionals using its products, employees, the communities where its people work and live, and its stockholders. Johnson & Johnson's public responsibility ultimately proved to have a positive public relations event and was the key to the Tylenol brand's survival.

Setting the Tone at the Top

The board and management demonstrate the importance of integrity and ethical values to support the functioning of internal control. Together they set their expectations that values, philosophy, and operating style will be followed. Some of the documents where this is evident include:

- **Mission and values statements**
- **Standards or codes of conduct**
- **Policies and practices**
- **Operating principles**
- **Directives, guidelines, and other supporting communications**
- **Timely inquiries and investigations into alleged conduct that is inconsistent with the code of conduct**
- **Actions and decisions of management at various levels and of the board of directors**
- **Prompt responses to deviations from expected standards of conduct**
- **Informal and routine actions and communication of leaders at all levels of the entity**

EXAMPLE

The executive director of a nonprofit organization wanted to find ways to instill the need for ethical behavior in its staff. Due to the type of entity and its activities, it was difficult to get people together in person. The organization started a monthly newsletter to communicate with not only the staff but also outsourced service providers, business partners and other parties to stress the importance of exercising sound integrity and ethical values. Each edition of the newsletter contained examples of ethical decision making along with a list of resources that could be accessed to discuss ethical decisions.

Establishing Standards of Conduct

The board's expectations of management for integrity and ethical values are defined in standards of conduct and understood at all levels. These standards of conduct guide the organization by:

- Establishing what is right and wrong
- Providing guidance for considering associated risks in navigating gray areas
- Reflecting legal and regulatory expectations by stakeholders
- Management is ultimately accountable for activities delegated to outsourced service providers. To ensure compliance with the entity's standards of conduct, they must be subject to oversight.

EXAMPLE

Management of a restaurant chain has created and maintains and distributes the code of conduct and ethical standards to all the employees. It was originally a model provided by a trade group but it was tailored to the entity. It is on the company's website. All of the employees are required to read it at the inception of their employment. And every year the employees go through a web-based training to further instill these values.

Since the restaurant business has a reputation of improper dealings with vendors and suppliers, the company also provides this code to the vendors as part of any agreement they sign with them.

The document focuses on the responsibility of the individual to identify and report breaches of the code of conduct and provides directions on how to report any suspicious behavior or violations observed.

Senior management reviews this document annually with the board and they discuss any risks to the entity. The code of conduct is revised when there are changes in laws or regulations or new modes of doing business.

Management's philosophy and operating style significantly impact the Control Environment because of its visibility. This could be reflected several ways by:

- Management's attitude about risk management – ranging from comprehensively identifying and mitigating risk or to routinely ignoring potential risk until it becomes an imminent threat.
- Management's philosophy toward regulatory reporting – such as tax evasion to overly-aggressive tax positions or such as taking aggressive financial accounting positions.
- Management's operating style for meeting budgeted sales, expense, and profits – how frequently it reviews actual versus budget performance, implementing

legitimate operating actions in response to below-budget performance, responding with threats and punishment to below-budget performance.

- Management's action for improper employee behavior – ranging from minimal or severe penalties or lack of publicity versus full disclosure for wrongdoing.

EXAMPLE

An accounts payable clerk identified a high-producing sales representative who regularly improperly inflated their expense reports. Degrees of management action in order of increasing severity could be to:

- ignore the situation
- tell the sales rep not to do it again
- deduct the overcharge from the expense reimbursement payment
- have the sales rep pay back cumulative historical overcharges
- terminate the sales rep with severance
- terminate the sales rep for cause without severance
- terminate the sales rep for cause without severance and make a company announcement
- terminate the sales rep for cause without severance and make a company announcement and prosecute for theft

Management's action not only would indicate its overall commitment level to integrity and ethics but also have a specific impact on the control environment. Inaction would significantly weaken the Control Environment by rendering control compliance or policy & procedure adherence meaningless. Worse, this may spread to other parts of the organization beyond the sales department or expense reporting, such as to inventory controls which may result in inventory shrinkage.

Indicators of a weak Control Environment may manifest itself in several ways:

- Low employee morale
- Unfilled open positions existing for in inordinately long period of time
- Higher employee turnover, especially in the finance and accounting department
- Reduced or negative sales growth
- Higher product returns
- Lower number of new product launches
- More frequent missed customer delivery dates
- Higher product warranty costs
- Slower accounts receivable collections
- Longer time to complete the monthly accounting close

Management Evaluates Adherence to Standards of Conduct and Addresses Deviations in a Timely Manner

- Management should have processes in place to evaluate conformity of individuals and teams to the standards of conduct. Some red flags that may indicate a lack of adherence to standards are:
  - Tone at top does not effectively convey expectations
  - Board does not provide impartial oversight of management
  - Decentralization without adequate oversight
  - Coercion by superiors, peers, or external parties
  - Performance goals that create pressure to cut corners
  - Inadequate channels for employee feedback
  - Failure to remedy non-existent or ineffective controls
  - Inadequate complaint response process
  - Weak internal audit function
  - Inconsistent, insignificant, or unpublicized misconduct penalties
- Deviations from the standards of conduct are identified and remedied timely and consistently, using a process that includes:
  - Defining a set of indicators to identify issues and trends related to the standards of conduct
  - Establishing continual and periodic compliance procedures to confirm that expectations and requirements are being met
  - Identifying, analyzing, and reporting business conduct issues and trends to senior management and the board
  - Evaluating the strength of leadership in the demonstration of integrity and ethical values for performance reviews, compensation, and promotions
  - Compiling allegations centrally and have them independently evaluated
  - Investigating allegations using defined investigation protocols
  - Implementing corrections timely and consistently
  - Periodically reviewing issues; searching for causes in order to modify policy, communications, training or controls

EXAMPLE

A trade group has policies and procedures to address illegal acts and other violations of the code of ethics such as kickbacks to suppliers or theft. The policy states that if such an act is identified it is investigated and if it is confirmed then the entity will terminate the person, revoke access privileges and then file charges with the appropriate authorities. The human resources manager will document these steps and then analyze the root cause of the issue and implement steps to avoid its recurrence. The audit committee gets this report.

An instance of violation was identified by an employee where an employee was obtaining free lodging and other benefits from a hotel chain for referring three of the group's conferences there. The policy clearly states that employees are not permitted to accept gifts over $25 from vendors and that all benefits such as free lodging would be the property of the trade group. The person who received the kickback was a senior level operations employee who had been with the organization for 15 years. This did not deter the entity from terminating the person.

Principle 2 – The Board of Directors Demonstrates Independence from Management and Exercises Oversight of the Development and Performance of Internal Control – Board of Directors Governance

Principle 2 separates board governance from management and requires that the board of directors:

- Define the board's governance roles and responsibilities
- Define the board's oversight and monitoring responsibilities for the organization's internal control structure
- Operate independently from management

COSO defines governance as the act or process of providing oversight, authoritative direction, or control. It differentiates power and responsibility among the board of directors and management by defining between what the board and executive management each do in providing direction and oversight over the organization's affairs.

Corporate governance is typically the board of directors' domain. The board of directors has a separate and distinct role from executive management in governing the organization. The board approves strategic decisions, establishes appropriate boundaries, oversees execution, and ensures accountability, fairness and transparency in the organization's relationships with its various stakeholders (shareholders, lenders, customers, suppliers, employees, governments, regulators, and the communities in which it operates).

Executive management aligns strategy, processes, people, reporting, and technology to accomplish the organization's mission in accordance with its established values. An important aspect of delineating responsibilities between the board and management is **setting boundaries**, which provide a broad context for balancing the organization's objectives and performance goals for creating enterprise value with the policies, processes, and control systems deemed appropriate to preserve enterprise value.

Boundaries are important because the board communications to the CEO set performance expectations that define success from a stakeholder perspective. The board also sets strategic boundaries around the decisions a CEO may make. The CEO provides leadership to focus the organization from a strategic, operational, and financial standpoint.

Boundaries have strategic importance as they reduce the risk of strategic drift leading to a lack of focus in managing the organization's risk profile. They also allow for faster decision-making and help to avoid wasted effort on initiatives that are not likely to achieve approval because they are off-strategy.

Board of Directors

The board of directors needs to demonstrate independence from management. In auditing and financial reporting, the definition of independence is a lack of a financial interest directly in the entity or indirectly in the entity's success.

Accordingly, the board needs to perform a periodic independence conflict-of-interest review about affiliations, relationships, and transactions with the organization that could impair independence. The board needs to accept its oversight responsibilities and exercise oversight of internal control development and performance.

The board makeup of number of directors, individual background, skills, and expertise need to be appropriate to reflect the organization's nature. Furthermore, the board should regularly self-evaluate whether its member background, skills, and expertise to ask management pertinent questions and respond appropriately. In addition members should regularly complete regular training to maintain their skills and expertise.

Based on its experience working with boards of directors, Deloitte published The Risk Intelligent Enterprise in 20148. According to Deloitte, governance and value creation are inseparable; however, too many companies view these as two opposed roles. Every decision, activity, and initiative that aims to create or protect value involves some degree of risk. Thus, effective risk governance calls for embedding appropriate risk management procedures into all of an organization's business pursuits.

Deloitte's Risk Intelligent Enterprise concept, illustrated as a pyramid below, integrates nine fundamental principles related to board of directors, senior management, and business unit leaders into a cohesive risk management framework. The board's risk governance sits at the top of Deloitte's framework as it guides all of the organization's risk management efforts.

Deloitte's nine fundamental principles of a Risk Intelligent program follow. This section focuses on the first four principles under Oversight at the top of the pyramid. The remaining five principles will be discussed in the Risk Management section.

[8] https://www2.deloitte.com/content/dam/Deloitte/za/Documents/governance-risk-compliance/ZA_RiskIntelligentEnterprise_24032014.pdf

Oversight

1. In a Risk Intelligent Enterprise, a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization.

2. In a Risk Intelligent Enterprise, a common risk framework supported by appropriate standards is used throughout the organization to manage risks.

3. In a Risk Intelligent Enterprise, key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organization.

4. In a Risk Intelligent Enterprise, a common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.

Common Risk Infrastructure

1. In a Risk Intelligent Enterprise, governing bodies (e.g., boards, risk committees, audit committees, etc.) have appropriate transparency and visibility into the organization's risk management practices to discharge their responsibilities.

2. In a Risk Intelligent Enterprise, executive management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program.

3. In a Risk Intelligent Enterprise, business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.

Risk Processes

1. In a Risk Intelligent Enterprise, certain functions (e.g., Finance, Legal, Tax, IT, HR, etc.) have a pervasive impact on the business and provide support to the business units as it relates to the organization's risk program.

2. In a Risk Intelligent Enterprise, certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organization's risk program to governing bodies and executive management.

The Board's Risk Oversight Role

Effective oversight begins with a solid mutual understanding of the extent and nature of the board's responsibilities versus management's and other stakeholder's. Key board-level responsibilities include setting the expectations and tone, establishing priorities, and initiating the communication and activities that constitute intelligent risk management. The ultimate goal is to assist management in creating a cohesive process in which risks and their impacts are routinely identified, evaluated, and addressed.

Board actions that define its oversight role:

- Define the board's governance roles and responsibilities

  Although the entire board is accountable for oversight, it may delegate responsibility for risk oversight to the risk committee. Having various committees play complementary oversight roles (e.g. risk committee, audit committee, compensation committee, etc.), and sharing their findings and insights with each other and the entire board, can help set the tone that risk oversight is important to all board and committee members. Even in boards where the nominal risk oversight responsibility rests with a single committee all board members should recognize that risk oversight is broader than that single committee. In any case, all such roles and responsibilities should be formally defined and clearly understood.

- Board composition

  A board should possess enough collective knowledge and experience to promote a broad perspective, open dialogue, and useful insights regarding risk. The board should perform a periodic evaluation, often carried out by the nominations committee, of the board's overall composition as well as each member's experiences, knowledge, and special characteristics and qualities. Having the right mix of board members at the table will allow for discussions that are founded on knowledge and perspective.

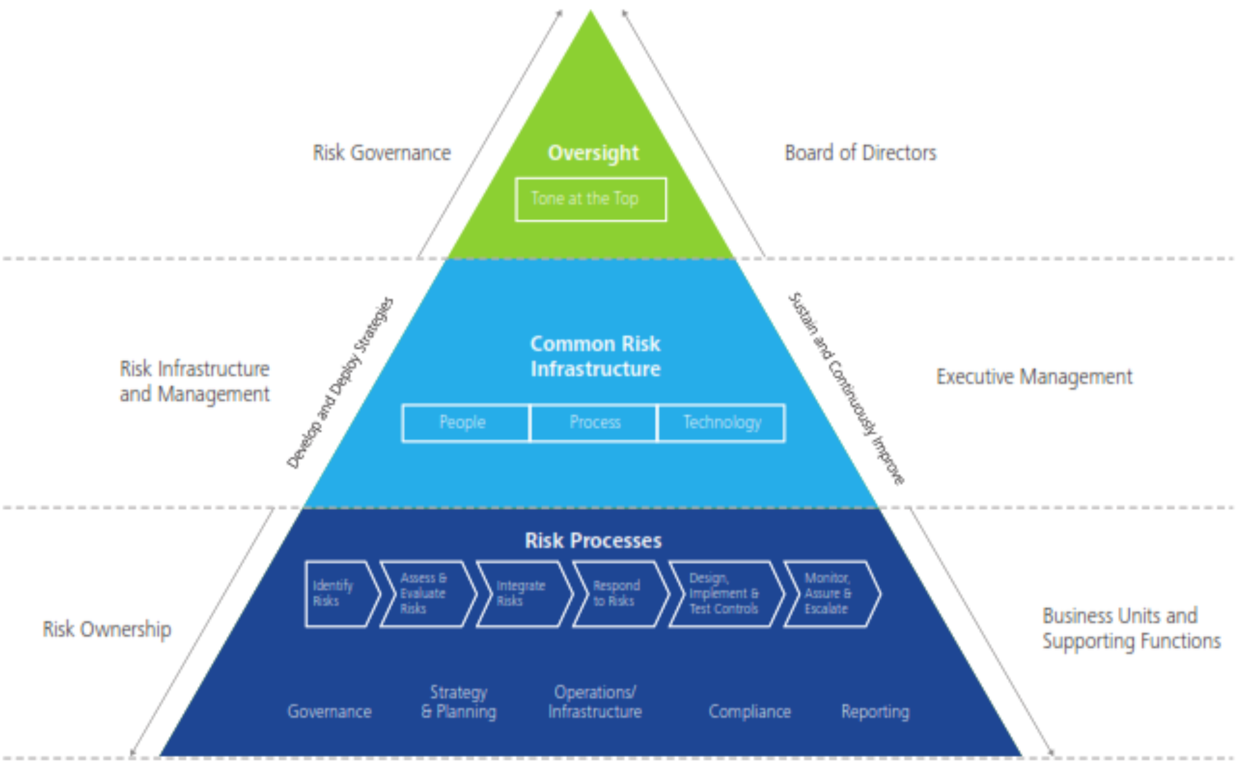
- Establish an enterprise-wide risk management framework

  Like any organizational process, risk management requires a framework that defines its goals, roles, activities, and desired results. The framework will help management establish goals, terms, methods, and measures, as well as gauge the need for specific programs (such as a contract risk and compliance program or training programs on risk awareness).

- Perform site visits

  Board members should visit the organization's facilities to enhance its understanding of work processes and the risks associated with value creation and preservation. A number of boards today are indeed using site visits to broaden their knowledge of, and demonstrate their interest in, the work of the enterprise.

The Risk Intelligent Enterprise


Risk Governance
Oversight
Tone at the Top
Board of Directors
Risk Infrastructure and Management
Develop and Deploy Strategies
Common Risk Infrastructure
People
Process
Technology
Sustain and Continuously Improve
Executive Management
Risk Ownership
Risk Processes
Identify Risks
Assess & Evaluate Risks
Integrate Risks
Respond to Risks
Design, Implement & Test Controls
Monitor, Assure & Escalate
Governance
Strategy & Planning
Operations/ Infrastructure
Compliance
Reporting
Business Units and Supporting Functions

Audit Committee

Public company audit committee guidance applies to private companies as well. In March 2017, Securities and Exchange Commission (SEC) Chief Accountant Wesley Bricker discussed how audit committees can effectively discharge their oversight responsibilities. Mr. Bricker said, "Audit committees also play a critical role in contributing to financial statement credibility through their oversight and resulting impact on the integrity of a company's culture and internal control over financial reporting (ICFR), the quality of financial reporting, and the quality of audits performed on behalf of investors."[9]

Mr. Bricker's speech highlighted seven areas in which audit committees can improve in their oversight of a company's financial reporting which will result in high-quality financial reporting.

1. Understand the organization's operating environment

   Audit committees should understand the businesses they serve and the impact of the operating environment (economic, technological, and societal changes) on corporate strategies. This establishes a frame of reference for the audit committee to evaluate its oversight scope and focus. Following are risks:

[9] https://www.sec.gov/news/speech/bricker-university-tennessee-032417

- Changes in the operating environment can result in changes in competitive pressures and different financial reporting risks

- Significant and rapid expansion of operations can strain controls and increase the risk of breakdown in controls

- Entering into industries, business areas or transactions with which an entity has little experience may introduce new risks associated with financial reporting

- Implementing new GAAP standards may affect risks in preparing financial statements, particularly if implementation planning or execution is lacking

2. Promote board diversity

   Diversity increases audit committee effectiveness. Diversity of thoughts diminishes the extent of group thinking. Also, diversity of relevant skills enhances the audit committee's ability to monitor financial reporting.

3. Balance the audit committee workload and keep current on financial reporting developments

   There are concerns about the capacity of audit committees to balance their workloads because of many demands on their time. Audit committee workload includes its core responsibilities plus emerging areas, such as cybersecurity and enterprise risk management (ERM). Boards of directors should consider whether they are identifying and managing risks of audit committee overload.

   Audit committees should attend training programs to help their members stay current on accounting and financial reporting developments, especially new accounting standards that have a significant effect.

4. Set a positive tone at the top and culture

   A strong control environment is especially important because new accounting standards require management to make more judgments than they have in the past. Audit committees may directly affect the control environment, which influences the behavior of management and other personnel.

   Tone at the Top is the foundation for effective internal controls. Audit committees can focus on tone and culture by working with management to obtain a clear and common understanding of what tone means, why tone is important, and what mechanisms are in place to assess the adequacy of the control environment, including across any relevant divisions and geographies. Also, it is critical for audit committees to discuss tone with the external auditor.

5. Understand disclosure controls and procedures over non-GAAP financial measures

   Audit committees need to oversee management's process and controls to calculate non-GAAP and other key operational measures, which includes:

   - Procedures in place over calculation accuracy and the consistency of the measures with those provided in prior periods

- Any non-GAAP policies that exist. If no policies exist, management needs to design and implement policies

- The individuals responsible for administering any non-GAAP policy, the number of times they approved reporting changes, and the reasons for reporting changes

6. Monitor corporate objectives that could conflict with effective oversight of external auditors

   Audit committees should work with other board committees to make sure important corporate objectives, such as cost reduction plans, are not implemented in ways that might adversely affect management's financial reporting responsibilities or inappropriately limit the scope of the external audit, the engagement terms, or the auditor's compensation. Audit committee responsibilities include the authority and responsibility to directly oversee auditor engagement terms, scope, and compensation.

7. Enhanced voluntary audit committee reporting

   Audit committees should continue to review their audit committee disclosures and consider whether providing additional insight into how the audit committee executes its responsibilities would make the disclosures more effective in communicating with investors

   Where there is a board and an audit committee, each should perform duties consistent with those structures, as defined by best practices. Basic oversight practices are:

   - An audit committee charter outlining its duties and responsibilities.

   - The board of directors should evaluate whether the audit committee has adequate resources and authority to conduct its duties and responsibilities.

   - The audit committee performs informed and diligent oversight of the financial reporting process, risk management, technology, and internal control structure that encompasses all five COSO internal control components.

   - The audit committee maintains direct communication with the independent external auditor and, if it exists, the organization's internal audit department.

   - The audit committee remains knowledgeable about the organization's existing internal control structure and current internal controls in industry.

   - The audit committee is current on recent regulatory changes and accounting standards and updates that impact the organization's internal control structure.

Audit Committee Leading Practices

Audit committees have full agendas and require careful planning to focus on critical priorities. Based on Deloitte's Audit Committee Resource Guide[10], following are audit committee leading practices to help them stay on track and execute their oversight responsibilities more effectively. The list is not all-inclusive, and certain activities may be the responsibility of the full board or another committee.

1. Audit committee composition and effectiveness

   - Focus on committee composition, including members' independence, financial literacy, and expertise.

   - Focus on having the right skills and experience on the audit committee, such as financial, industry, risk management, business, and leadership experience.

   - Limit the number of audit committee members to four or five to optimize effectiveness.

   - Consider rotating audit committee members periodically, including the chairman.

   - Develop a succession plan for audit committee members and a rotation plan for the chairman, in coordination with the nominating committee.

   - Review and approve the audit committee charter and align activities with a calendar that sets forth required activities and allows flexibility for additional topics.

   - Perform a robust self-assessment annually.

   - Discuss the results of the self-assessment with the audit committee in an executive session and develop tactical plans to address findings.

2. Audit committee meeting effectiveness

   - Review and approve the audit committee charter and develop a calendar that incorporates required activities and allows flexibility for additional topics.

   - Develop meeting agendas in consultation with management; resist the urge to reuse past agendas without discussion.

   - Align audit committee meeting materials and agendas with priority areas.

   - Distribute briefings and other materials well in advance of meetings.

   - Include executive summaries to reports that highlight issues and critical discussion points and allow discussion versus presentation during meetings.

[10] Bujno, M., Hitchcock, C., Parsons, K., and Lamm, B. (2018). Audit Committee Resource Guide. Retrieved from https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/audit-committee-resource-guide.html.

- Consider a regular "watch list" to report on ongoing topics even when they are not the focus of a particular meeting.

- Foster an environment where open dialogue and candid discussions are encouraged.

- Hold executive sessions at every meeting with the CFO, internal auditors, and independent auditors; consider having the committee meet after the executive sessions to discuss the effectiveness of the meeting and future agenda items.

3. Audit committee member orientation and education

   - Provide orientation of new members that focuses on audit committee responsibilities and involves committee members, the CEO, the CFO and finance management, internal audit, and the independent auditor.

   - Address board education in the company's corporate governance guidelines in a way that is consistent with NYSE listing standards.

   - Include educational topics on the agendas once or twice a year; topics may include a deep dive on a specific area of the business and related risks or a refresher on a significant accounting estimate.

   - Offer annual continuing education opportunities in financial reporting and other areas relevant to the audit committee, such as specialized industry matters, new regulations, operations, and emerging topics such as cyber risk.

   - Oversight of internal controls and financial reporting

   - Understand risk areas as assessed by management, the internal auditors, and the independent auditor, as well as related controls. Also understand any prior internal control issues and how they have been resolved.

   - Understand the design and components of the company's antifraud and anticorruption compliance programs and confirm that those programs have sufficient oversight, autonomy, and resources.

   - Understand complex accounting and reporting areas and how management addresses them.

   - Understand significant judgments and management estimates and their impact on the financial statements.

   - Consider conducting a periodic analytic review of balance sheet items, focused on key underlying assumptions and potential vulnerabilities.

   - Be aware of any uncertain tax positions taken by the company and their potential impact on financial reporting.

   - Stay abreast of pending financial reporting and regulatory developments and understand how they may affect the company.

  - Understand the issues raised in SEC comment letters received by the company, as well as management's response.

  - Consider the nature of SEC comment letters issued to companies in similar industries.

  - Consider levels of authority and responsibility in areas such as pricing and contracts, acceptance of risk, commitments, and expenditures.

4. Risk oversight

   - Focus on financial risk oversight and assessment and understand financial risk management policies and processes.

   - Avoid becoming overly dependent on checklists for monitoring financial risk.

   - Periodically reassess the list of top risks, including which member of management and which board committee is responsible for each.

   - Evaluate IT projects and related risks, particularly those with financial statement impact.

   - Consider post-acquisition reviews to evaluate the reliability of initial acquisition assumptions and make adjustments to future acquisitions if necessary.

   - Have appropriate business leaders periodically provide an overview of their business, focusing on financial risks and other factors that may influence the financial statements.

   - Periodically visit company locations and meet with local management.

   - Communicate the company's financial risk story to stakeholders.

   - Understand the issues raised in SEC comment letters received by the company, as well as management's response.

   - Understand the company's strategy for managing tax risk, tax controversy, and volatility in the effective tax rate.

   - Consider potential reputational risks associated with tax positions.

5. Ethics and compliance

   - Focus on the tone at the top, culture, ethics, and hotline monitoring.

   - Provide oversight of compliance with the company's code of ethics and compliance.

   - Initiate internal or independent investigations on matters within the committee's scope of responsibility.

- Understand the risk and mitigation mechanisms with regard to management override of controls.

- Periodically meet with those responsible for overseeing ethics and compliance matters in executive sessions.

6. Interaction with the internal auditors

   - Provide the internal auditors with direct access to the audit committee.

   - Consider having internal audit report directly to the audit committee and administratively to senior management.

   - Play an active role in determining the highest and best use of internal audit, as well as the appropriate structure of the group (e.g., in-house versus outsourced resources).

   - Be involved with the internal audit risk assessment and audit plans, including activities and objectives regarding internal control over financial reporting.

   - Conduct annual evaluations of the chief audit executive.

   - Understand internal audit staffing, funding, and succession planning, particularly the adequacy of resources; consider performing peer benchmarking to compare relevant metrics.

7. Interaction with the independent auditor

   - Exercise ownership of the relationship with the independent auditor.

   - Focus on the independent auditor's qualifications, performance, independence, and compensation, including a preapproval process for audit and nonaudit services.

   - Get to know the lead audit partners and meet periodically with specialists (e.g., tax, IT, actuarial, SEC).

   - Establish expectations regarding the nature and method of communication, as well as the exchange of insights.

   - Set an annual agenda with the independent auditor and engage in regular dialogue beyond audit committee meetings.

   - Provide formal evaluations and regular feedback.

8. Coordination and communication with the full board and its other committees

   - Understand areas of risk and responsibilities delegated to other committees.

   - Coordinate with the compensation committee on incentive goals for the talent pool.

- Coordinate with the compensation committee to establish the financial metrics used in incentive compensation plans.

- Work with the compensation committee to understand the implications of the incentive structure, including its impact on employee retention and potential increases in fraud risk.

- Increase focus on the compensation of officers and directors, including the appropriate use of corporate assets.

- Coordinate with the nominating committee to develop succession plans for audit committee members and the chairman.

EXAMPLE - SAMPLE AUDIT COMMITTEE CHARTER

This sample audit committee charter is based on Deloitte's observations of selected companies and the requirements of the SEC, the NYSE, and NASDAQ.

Audit committee of the board of directors—charter

I. Purpose and authority

The audit committee is established by and among the board of directors for the primary purpose of assisting the board in:

- Overseeing the integrity of the company's financial
- Overseeing the company's compliance with legal and regulatory requirements
- Overseeing the registered public accounting firm's (independent auditor's) qualifications and independence
- Overseeing the performance of the company's independent auditor and internal audit function
- Overseeing the company's systems of disclosure controls and procedures
- Overseeing the company's internal controls over financial reporting
- Overseeing the company's compliance with ethical standards adopted by the company

The audit committee should encourage continuous improvement and should foster adherence to the company's policies, procedures, and practices at all levels. The audit committee has the authority to conduct investigations into any matters within its scope of responsibility and obtain advice and assistance from outside legal, accounting, or other advisers when necessary to perform its duties and responsibilities.

In carrying out its duties and responsibilities, the audit committee has the authority to engage outside legal, accounting, or other advisers, and to seek any information it requires from employees, officers, and directors.

The company will provide appropriate funding, as determined by the audit committee, for compensation to the independent auditor, to any advisers that the audit committee chooses to engage, and for payment of ordinary administrative expenses of the audit committee that are necessary or appropriate in carrying out its duties.

The committee's principal responsibility is one of oversight. The fundamental responsibility for the company's financial statements and disclosures rests with management and the independent auditor.

II. Composition and Meetings

The audit committee will comprise three or more directors as determined by the board.

Committee members will be appointed by the board at the annual organizational meeting of the board to serve until their successors are elected. Unless a chairman is elected by the full board, the members of the committee may designate a chairman by majority vote.

Each audit committee member will meet the applicable standards of independence and the determination of independence will be made by the board and as defined by applicable standards listing.

To help meet these requirements, the audit committee will provide its members with annual continuing education opportunities in financial reporting and other areas relevant to the audit committee.

The board will determine that a director‘s simultaneous service on multiple audit committees will not impair the ability of such member to serve on the audit committee. The committee will meet at least quarterly, or more frequently as circumstances dictate. The committee chairman will approve the agenda for the committee‘s meetings and any member may suggest items for consideration. Briefing materials will be provided to the committee as far in advance of meetings as practicable.

Each regularly scheduled meeting will conclude with an executive session of the committee absent members of management. As part of its responsibility to foster open communication, the committee will meet periodically with management, the director of the internal audit function, and the independent auditor in separate executive sessions.

III. Responsibilities and Duties

To fulfill its responsibilities and duties, the audit committee will:

Documents/reports/accounting information review

Review this charter at least annually and recommend any necessary amendments to the board of directors.

Meet with management and the independent auditor to review and discuss the company‘s annual financial statements and quarterly financial statements prior to the company‘s Form 10-K and 10-Q filings or release of earnings, including the company‘s disclosures under “Management‘s Discussion and Analysis of Financial Condition and Results of Operations”. Review internal control reports, other relevant reports or financial information submitted by the company to any governmental body or the public, and relevant reports rendered by the independent auditor.

Review internal control reports, other relevant reports or financial information submitted by the company to any governmental body or the public, and relevant reports rendered by the independent auditor.

Discuss the listed company’s earnings press releases, as well as financial information and earnings guidance provided to analysts and rating agencies, including the type and presentation of information, paying particular attention to any pro forma or adjusted non-GAAP information. Such discussions may be in general terms (i.e., discussion of the types of information to be disclosed and the type of presentations to be made).

Review the regular internal reports to management prepared by the internal audit function, as well as management‘s response.

Independent Auditor

Appoint (and recommend that the board submit for shareholder ratification, if applicable), compensate, retain, and oversee the work performed by the independent auditor retained for the purpose of preparing or issuing an audit report or related work, including the resolution of disagreements between management and the independent auditor regarding financial reporting.

Review the qualifications and independence of the independent auditor and remove the independent auditor if circumstances warrant. The independent auditor will report directly to the audit committee.

Review and preapprove both audit and non-audit services to be provided by the independent auditor. The authority to grant preapprovals may be delegated to one or more designated members of the audit committee, whose decisions will be presented to the full audit committee at its next regularly scheduled meeting.

Consider whether the auditor‘s provision of permissible non-audit services is compatible with the auditor‘s independence.

Actively engage in dialogue with the independent auditor with respect to any disclosed relationships or services that may affect the independence and objectivity of the auditor and take appropriate actions to oversee the independence of the independent auditor.

Discuss with the independent auditor the matters required to be discussed under the standards of the PCAOB.

Review with the independent auditor any problems or difficulties encountered during the course of the audit, including any restrictions on the scope of the independent auditor’s activities or on access to requested information, and any significant disagreements with management, together with management’s response.

Hold timely discussions with the independent auditor regarding the following:

- All critical accounting policies and practices
- All alternative treatments of financial information within generally accepted accounting principles related to material items that have been discussed with management, ramifications of the use of such alternative disclosures and treatments, and the treatment preferred by the independent auditor
- Other material written communications between the independent auditor and management, including, but not limited to, the management letter and schedule of unadjusted differences.
- At least annually, obtain and review a report by the independent auditor describing:
- The independent auditor‘s internal quality-control procedures
- Any material issues raised by the most recent internal quality control review or peer review, or by any inquiry or investigation by governmental or professional authorities within the preceding five years with respect to independent audits carried out by the independent auditor, and any steps taken to deal with such issues
- All relationships between the independent auditor and the company

Review the experience and qualifications of the lead partner each year and determine that all partner rotation requirements, as promulgated by applicable rules and regulations, are executed. The audit committee should present its conclusions to the full board.

Set policies, consistent with governing laws and regulations, for hiring personnel of the independent auditor.

Financial reporting processes, accounting policies, and internal control structure

In consultation with the independent auditor and the internal audit function, review the integrity of the company‘s internal and external financial reporting processes.

Understand the scope of the audit plan, including the independent auditors’ review of internal control over financial reporting. Receive and review any disclosure from the company‘s CEO and CFO made in connection with the certification of the company‘s quarterly and annual reports filed with the SEC of:

- significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the company‘s ability to record, process, summarize, and report financial data; and
- any fraud, whether or not material, that involves management or other employees who have a significant role in the company‘s internal controls.

Review major issues regarding accounting principles and financial statement presentations, including any significant changes in the company‘s selection or application of accounting principles; major issues as to the adequacy of the company‘s internal controls; and any special audit steps adopted in light of material control deficiencies.

Review analyses prepared by management and the independent auditor setting forth significant financial reporting issues and judgments made in connection with the preparation of the financial statements, including analyses of the effects of alternative GAAP methods on the financial statements.

Review the effect of regulatory and accounting initiatives, as well as off-balance-sheet structures, on the financial statements of the company.

Review and approve all related-party transactions, defined as those transactions required to be disclosed. Discuss with the independent auditor its evaluation of the company‘s identification of, accounting for, and disclosure of its relationships with related parties as set forth under the standards of the PCAOB.

Establish and oversee procedures for the receipt, retention, and treatment of complaints regarding accounting, internal accounting controls, or auditing matters, including procedures for confidential, anonymous submissions by company employees regarding questionable accounting or auditing matters.

Internal Audit

Review and advise on the selection and removal of the internal audit director.

Review the activities and organizational structure of the internal audit function, as well as the qualifications of its personnel.

Annually, review and recommend changes (if any) to the internal audit charter.

Periodically review, with the internal audit director, any significant difficulties, disagreements with management, or scope restrictions encountered in the course of the function‘s work.

Periodically review, with the independent auditor, the internal audit function‘s responsibility, budget, and staffing.

Ethical Compliance, Legal Compliance, and Risk Management

Oversee, review, and periodically update the company‘s code of business conduct and ethics and the company‘s system to monitor compliance with and enforcement of this code.

Review, with the company‘s counsel, legal compliance and regulatory matters that could have a significant impact on the company‘s financial statements.

Discuss policies with respect to risk assessment and risk management, including appropriate guidelines and policies to govern the process, as well as the company‘s major financial risk exposures and the steps management has undertaken to control them.

Consider the risk of management‘s ability to override the company‘s internal controls.

Reporting

Report regularly to the board regarding the execution of the audit committee‘s duties, responsibilities, and activities, any issues encountered, and related recommendations.

Recommend to the board of directors that the audited financial statements be included in the company‘s annual report on Form 10-K.

Provide a report of the audit committee, which contains certain required disclosures, in the company’s annual proxy.

Other Responsibilities

Review, with management, the company‘s finance function, including its budget, organization, and quality of personnel.

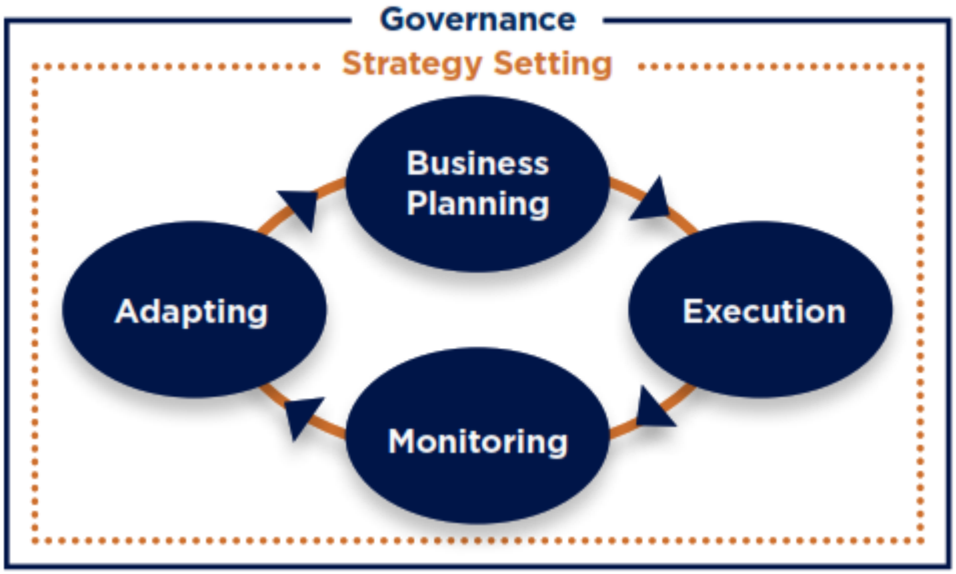
Conduct an annual performance assessment relative to the audit committee‘s purpose, duties, and responsibilities outlined herein.

Perform any other activities consistent with this charter, the company‘s bylaws, and governing laws that the board or audit committee determines are necessary or appropriate.

Improving Organizational Performance and Governance

The COSO framework can help improve organizational performance and governance.

In COSO’s February, 2014 publication, *Improving Organizational Performance and Governance*, it presented a simple holistic business model of governance and management processes, which is shown below.[11]



[11] https://www.coso.org/Documents/2014-2-10-COSO-Thought-Paper.pdf

"[COSO's] model begins with governance, which begins with the organization's vision and mission and consists of oversight from the board of directors of the enterprise's planning and operations. Also included are the activities of executive management in ensuring the effectiveness of strategy setting and the organization's other management processes.

Next is strategy setting, which is the process by which executive management (and, depending on the size of the enterprise, the board of directors) articulates a high-level plan for achieving one or more goals consistent with the organization's mission. Together, the two elements of governance and strategy setting provide direction to the enterprise and clearly have a place in ensuring the organization's success in meeting the demands and expectations of stakeholders.

Inside the business model are four elements based on Dr. Edwards Deming's iterative four-step management method used in business for control and continuous improvement of "Plan, Do, Check, Act". COSO repurposed these four elements as business planning, execution, monitoring and adapting. These elements represent what operating management does in executing the strategy approved by executive management and the board.

The six attributes of the contextual business model shown above are further described below:

- **Governance** is the act or process of providing oversight, authoritative direction, or control. It can also be the allocation of power among the board, management, and shareholders. It is often applied to describing what the board of directors and executive management does in providing direction and oversight to the organization's affairs. Corporate governance is the board's domain and refers to the framework of rules and practices by which a board oversees strategy setting and organizational management.

  Effective governance ensures accountability, fairness, and transparency in the organization's relationships with its stakeholders (shareholders, lenders, customers, suppliers, employees, governments, regulators, and the communities in which it operates.

- Strategy setting sets the context for business planning by providing management's high-level plan for what the organization seeks to achieve over its selected strategic planning horizon, including its overall direction, environmental scan, differentiating capabilities, and the infrastructure needed to make the differentiating capabilities a marketplace reality. Strategy is often presented in the form of overall goals, initiatives, and tactics.

The management cycle for delivering the strategy is a continuing ongoing dynamic process made up of four components:

- **Business planning** formally articulates specific goals or roadmaps on how operating management will contribute to achieving the overall strategic objectives, explains why those objectives are achievable, and provides an enabling process for the organization within the specific planning horizon. Business planning achieves the following:

  - Links the traditional processes of strategic planning, risk mitigation, budgeting, forecasting, and resource allocation.

  - Breaks down the corporate strategy into achievable plans, with financial and operational targets, including key performance indicators (KPIs) and key risk indicators (KRIs), to establish management accountability for results.

  - Aligns business objectives, key metrics, plans, and budgets across the organization down to the level of greatest achievability and accountability. It also engages the appropriate manager with the resources needed to implement strategic objectives. This is typically called an operating plan.

- **Execution** consists of the organization's core operations in place to design, build, and operate the processes that make the business plan work and that deliver expected performance in accordance with the organization's values and strategy.

- **Monitoring** consists of the activities established by management to review and oversee execution of the organization's operations against the overall strategic plan, including the level of acceptable risk. Monitoring activities consider both

  - performance metrics that demonstrate progress towards achievement of business objectives and long-term strategic goals, and

  - risk metrics to ensure risk remains at acceptable levels. They are focused both externally and internally to scan for economic, competitor, regulatory, and other developments and trends.

  Monitoring focuses both externally and internally to identify economic, competitive, regulatory, and other development and trends.

- **Adapting** describes the organizational processes by which issues identified through monitoring activities as requiring management follow-up and corrective action are translated into implementable changes to the corporate strategy, business plan, or execution tactics. This includes risk responses and internal controls.

  Adapting is important when considering the organization's resiliency and agility that is so vital to success in a rapidly-changing business environment. It includes process improvements to close performance gaps related to stakeholder expectations and competitors as well as mid-course corrections in response to changes in the external and internal environments that alter assumptions underlying the strategy and business plan.

These six elements provide an illustrative structure for demonstrating how the COSO frameworks contribute value to the overall organization's governance and management processes."[12]

[12] https://www.coso.org/Documents/2014-2-10-COSO-Thought-Paper.pdf

Principle 3 – Management Establishes, with Board Oversight, Structures, Reporting Lines, and Appropriate Authorities and Responsibilities in the Pursuit of Objectives

With board oversight, management establishes organization structures with position hierarchal reporting lines, authority by organization level and position, and responsibilities by position. The optimal organization structure differs by industry due to complexity, regulation, and best practices; and differs by organization size and legal structures. Large organizations require more formalized structure than small companies.

Strong organization structures reduce wrongdoing and fraud opportunities, compared with weak organization structures. Overly complex organization structures may inherently increase wrongdoing and fraud opportunities due to difficulty monitoring the business. Finally, centralized organization structures reduce wrongdoing and fraud opportunities compared with decentralized structures because it is easier to monitor controls.

COSO's focus points (to clarify what the principle is seeking to achieve) for this principle are:

- Considers all of the entity structures

  Entities may have multiple structures requiring different organizational relationships to support achieving their objectives. Examples are: operating units, product lines, ventures, legal entities, geographical locations, and outsourced service providers. Management needs to consider several variables when establishing organizational structures, such as:

  - Nature, size, and geographic distribution of the entity's business
  - Risks related to the entity's objectives and business processes
  - Nature of the assignment of authority
  - Definition of reporting lines
  - Financial, tax, regulatory, and other reporting requirements
  - Management and governance consider these variables and the risk when establishing or changing the organizational structure

- Establishes organizational structure reporting lines

  Each entity structure may need different reporting lines to optimize executing job responsibilities and authority levels. In addition, management designs and evaluates operating and financial information flows.

- Defines job responsibilities and authority level limits

The board and management determine authority level limits, define job responsibilities, and segregate duties for controls for the organization hierarchy levels. These hierarchy levels are: the board of directors, senior management, managers, employees, and outsourced service providers.

The board of directors delegates authority and defines and assigns responsibility. Key roles and responsibilities assigned typically include:

- Board stays informed and challenges senior management for guidance on significant decisions
- Senior management establishes directives, guidance, and control to enable staff to understand and carry out their duties
- Management executes senior management's directives
- Personnel understand standards and objectives for their area
- Management and responsible personnel oversee outsourced service providers

Authority empowers, but limitations of authority are needed so that:

- Delegation occurs only as required
- Inappropriate risks are not accepted
- Segregation of duties to reduce risk of inappropriate conduct
- Leverage technology as appropriate to facilitate defining and limiting roles and responsibilities
- Third-party service providers clearly understand the extent of their decision-making authority

Regardless of the size, strength, complexity, or centralization, management and employees must believe they are held accountable for achieving business strategic and operational objectives as well as for complying with organization policies & procedures, internal controls, and employee code of conduct.

Principle 4 – The Organization Demonstrates a Commitment to Attract, Develop, and Retain Competent Individuals in Alignment with Objectives - Commitment to Competence

Management must recruit, hire, and retain employees with the background, experience, knowledge, and technical skills to perform their job responsibilities. The required employee capabilities will differ by industry due to complexity, regulation, and best practices; and differs by organization size and legal structures. Large organizations generally require higher-level employee capabilities than smaller organizations.

The Institute of Management Accountants Statement of Ethical Professional Practice, issued in 2017, contains a competence standard which has three components.

1. Maintain an appropriate level of professional leadership and expertise by enhancing knowledge and skills.

2. Perform professional duties in accordance with relevant laws, regulations, and technical standards.

3. Provide decision support information and recommendations that are accurate, clear, concise, and timely. Recognize and help manage risk.

COSO's focus points for this principle are:

- Establishes employee competence policies and practices

  The board's and management's job responsibility and authority expectations determine competence required to achieve business objectives

- Evaluates employee competence and addresses weaknesses

  The board and management evaluate employee performance against job responsibilities, authority, and business objectives. They implement corrective action for weaknesses identified. This evaluation also includes outsourced service providers.

- Attracts, develops, and retains competent employees

  Management attracts competent employees to join the organization and retains them through training and mentoring. **This also applies to outsourced service providers**.

- Develops a succession plan

  The board and management prepare for employee promotions and departures by developing contingency plans for management succession. This ensures the internal controls structure is maintained in the event of management change.

Responsibility for management and employee competency rests with the human resources department. The human resources department establishes policies & procedures for hiring, developing, promoting, evaluating, compensating, disciplining, and terminating employees.

Internal controls require that all departments, not just finance and accounting, document policies & procedures in writing. Writing documents that a control exists (there are other indicators for control implementation and effectiveness). Written documentation also facilitates communication which improves the control environment, and became a COSO requirement with the 2013 update. For organizations that must have financial audits or regulatory audits, control documentation is important because it shows control existence. Periodic control evaluation and assessment documentation shows whether the implemented control is operating effectively.

The human resources department's role in the control environment comes from policies and procedures documentation, and communication. A policy and procedure needs a periodic written review to document that it is implemented and to assess its effectiveness. This is not unlike an employee performance review but does not occur as frequently.

A written position description and experience requirements demonstrates an organization's commitment to competency. It also establishes performance levels to measure responsibilities, authority, and accountability in achieving organization objectives. Communicating open positions supports retaining employees because employees can recognize opportunities. It also documents management's commitment to promote qualified existing employees.

Communicating open positions supports training by identifying and communicating desired competencies. Employees lacking certain competencies should seek training, which, when completed, increases the organization's overall employee competency level. In addition professional associations, such the IMA (mentioned above) and the American Institute of CPA's for accounting and finance professionals, require continuing professional education

Periodic employee performance appraisals increase communication and authenticates management's commitment to develop employees and to promote qualified employees into roles with greater responsibility and authority. On the other side of the coin, disciplinary action from poor performance reviews also communicates management's commitment to high competency levels. The board reviews the CEO's performance and should oversee the CEO's performance review of their direct reports.

Rewards of performance-based compensation increases or promotions to greater responsibility and authority enforce performance and behavior expectations. Disciplinary actions for poor performance communicate to all employees that ethical lapses or behavioral differences with published employee code of conduct are not acceptable.

EXAMPLE

Periodic Performance Assessment

A software company periodically reviews the performance of employees with responsibility for owning, executing or testing controls over financial reporting. Performance expectations are set at the beginning of each year, and actual performance is evaluated versus those expectations. Progress is reviewed with employees each quarter, and more formally at year end. Career advancement is based on these performance ratings. Management identifies specific areas for improvement, and employees are expected to confer with their manager to agree on a training and development plan to address these areas.

Principle 5 – The Organization Holds Individuals Accountable for Their Internal Control Responsibilities in Pursuit of Objectives – Enforces Accountability

Too often in many companies, most of the organization believes that internal controls over financial reporting (ICFR) are strictly finance and accounting department concerns. Management must hold all employees accountable for control compliance (meaning effectiveness). Furthermore, many ICFR have process owners in other departments, such as human resources as discussed in COSO Principle 4. Thus, non-financial departments have accountability for control design, implementation, and effectiveness.

Thus, control environment effectiveness depends on all employees having internal control consciousness. Management needs to take action when controls are ineffective or employee performance is inadequate. Because actions speak louder than words, if management extols internal control and code of conduct compliance but does not reinforce good performance and more importantly punish bad performance, then the control environment becomes less effective. Worse, ignoring control compliance and operating performance results in low employee morale, which, in turn, produces poorer operating performance.

COSO's focus points for this principle are:

- Enforces accountability through organization structures, authority levels, and responsibilities

  Management develops employee control responsibility communication processes and measures employee performance against these responsibilities. Communication is an important control so that employees are aware of their accountabilities. In instances where performance is below standard because controls are either not implemented or not effective, management makes corrections.

  The Tone at the Top helps establish and enforce accountability, morale, and a common purpose through:

  - Clarifying expectations
  - Providing guidance through management philosophy and operating style
  - Control and information flow
  - Establishing anonymous or confidential communication channels for reporting ethical violations
  - Employee commitment toward collective objectives
  - Management's response to standards deviations

- Establishes and measures performance levels and incentives/disincentives for performance

Management establishes strategic (long term goals), operational (budgets), behavioral (employee code of conduct), and control performance levels. Management measures employee performance against these levels and appropriately rewards compliance/attainment or properly disciplines poor performance.

Good performance measures, incentives, and rewards support an effective system of internal control. Key success measures include:

- Clear objectives – consider all levels of personnel and the multiple dimensions of expected conduct and performance
- Defined implications – communicate objectives, review relevant market events, and communicate failure consequences
- Meaningful metrics – define metrics, measure expected versus actual performance, and assess the expected impact
- Adjustment to changes – regularly adjust performance measures based on continual risk/reward evaluation

■ Evaluates performance measures continuously

Management needs to continuously evaluate the organization's performance measures appropriateness for the organization's control objectives.

■ Identifies excessive pressures that could lead to wrongdoing

Management evaluates pressures on operational and financial goal achievement or responsibility fulfillment. Stretch goals are appropriate in any organization, but unattainable goal create disincentives and low morale which may lead to lower performance and encourage wrongdoing.

Excessive pressures can cause undesirable side effects. Excessive pressures are most commonly associated with:

- Unrealistic performance targets, especially short-term
- Conflicting objectives of different stakeholders
- Imbalance between rewards for short-term versus long-term objectives

■ Evaluates actual performance and provides rewards or disciplinary action

Management evaluates employee internal control and code of conduct responsibility compliance and provides rewards or disciplinary action.

EXAMPLE

Defining and Communicating the Basis for Reward

Plymouth Parts, a regional distributor of auto parts, has implemented a plan designed to identify control deficiencies as early as possible. This is done by providing departments with credit on their internal audit grade when they self-report deficiencies which they have identified, rather than waiting for the internal audit department to find the problem. The company's rewards system requires departments to achieve certain defined performance measures; reaching the target is easier for a department which has received an internal audit credit for self-reported control deficiencies, and a department's internal control score can affect its compensation and benefits.

Code of Conduct

An employee Code of Conduct is an important component of an organization's control environment. It communicates appropriate employee workplace business conduct and actions and, thus, reinforces the organization's values and ethics. A Code of Conduct is the organization's ethical standard, and the organization's reputation depends on each employee's compliance. Of course, it is not possible to provide clear direction for every situation; thus, employees also need to follow their common sense.

An employee Code of Conduct is narrowly focused on ethical behavior which makes it different than an Employee Handbook which is more broadly focused on company benefits, policies, and procedures.

A Code of Conduct's effectiveness depends on the CEO and executive management supporting it more than through words (lip service) but primarily through their actions. This is akin to Tone at the Top which is also discussed in this section. Visible responsible actions by senior leadership directly impacts how employees behave. Further reinforcement comes from enforcing consequences of employee code violations.

An employee Code of Conduct is narrowly focused on ethical behavior, which makes it different than an Employee Handbook, which is more broadly focused on company benefits, policies, and procedures. Thus, a Code of Conduct is much briefer. The Code of Conduct is generally provided in conjunction with an Employee Handbook.

The Code of Conduct needs to be recommunicated to all employees each year with employee-returned documentation that indicates that they read the Code and understand it. This documentation can be a written signature or electronic confirmation. A best practice is an on-line site that trains employees on the code, reinforces it through test questions, and captures this interaction as documentation confirmation.

Not having an employee Code of Conduct may expose the organization to legal risk. This is especially relevant if a company with an employee Code of Conduct disciplines an employee for an ethical violation. The employee may respond that they did not know they did not know what they did was not allowed.

EXAMPLE

A small company did not have an employee Code of Conduct. The owner believed that such a document was an unnecessary cost and burden to develop, print, and distribute.

A company employee had a side business selling pottery they made at home. The employee used the company computer systems and telephones for record-keeping and to contact customers. The information technology department detected access to non-business internet sites and identified the employee. In addition the information technology department performed a scan of the employee's company computer, email, and phone records that validated the non-company-business actions.

The employee's supervisor confronted the employee with the evidence as a part of documenting the activities in a disciplinary memorandum to be placed in the employee's personnel file. Instead of contrition, the employee was angry that the company had read her personal email and personal files, even though they existed on the company-provided computer and company network.

The employee retained an attorney who threatened legal action against the company taking the position that the employee had a legal expectation of privacy and the company violated the employee's privacy rights. Furthermore, the attorney said their client had no reason to know that they had done something wrong.

An employee Code of Conduct that established and communicated expected employee behaviors during office hours and that company resources could be used only for business would result in a different outcome to this situation. The employee Code of Conduct could also communicate that employees should not have expectations of privacy for company-owned resources of computers, network devices, and emails.

Conflict of Interest

A conflict of interest is a situation in which an individual has competing interests or loyalties. It creates risk that a person's judgment or actions for their primary responsibility may be unduly influenced by a secondary interest. An example would be a person who has a professional position of authority in one organization that conflicts with their personal interests or their professional interests in another organization.

Conflicts of interest exists when multiple interests potentially could corrupt their personal motivation or organization's interests. In this event, an employee is more influenced by their secondary interest over their primary interest which is their professional obligation. Controls are needed if circumstances exist that could reasonably create a risk that the employee's decisions may be unduly influenced by their secondary interests. Examples include:

- Self-dealing is when someone has a professional responsibility in an organization and has outside conflicting interests and their actions are more in their own self-interest rather than the interest of the organization.
- Nepotism is the practice of giving favors to relatives and close friends, often by hiring them.

These activities in themselves create the conditions for a conflict of interest, but not necessarily wrongdoing or criminal activity. For example, a business executive hiring their daughter might not be a conflict of interest unless the daughter is given preferential treatment, such as paying her a salary higher than others at her pay level or shorter working hours than other employees. If the executive isn't in a position to give favors, there's not a conflict of interest. However, it is very important to avoid the appearance of a conflict of interest, even if there is no true conflict.

Following are some workplace examples of conflicts of interest:

- An employee may work for one company but he or she may have a side business that competes with the employer. In this case, the employee would likely be asked to resign or be fired.

- A common workplace conflict of interest involves a manager and his or her employee who are married or dating and have a relationship. This is a conflict because the manager has the power to give raises or promotions to the employee. Discussions about the company between the two people may also breach confidentiality restrictions.

- An employee who has a friendship with a supplier and allows that supplier to go around the bidding process or gives the supplier the bid.

- A third-party supplier provides valuable gifts to company employees who are in a position to award the supplier with product of service business. Many companies require any gift to be valued at less than $35.

- A former employee may copy their employer's customer list or product price data before resigning and then competing directly. This is a reason that companies often require non-compete agreements as a condition of employment.

Boards of directors may also have conflicts of interests. Examples are:

- A board member may have a romantic relationship with an executive employee, or may have an ownership interest in a competing company. In these situations, the board member should resign.

- A board member may learn about a potential business transaction that might affect the company valuation (up or down). A board member's attempt to profit from this knowledge is insider trading which is both a conflict of interest and illegal.

- A board member may receive a loan or overdraft from the company.

- Non-profit boards have the same issues. In addition, the IRS requires non-profits disclose potential conflicts of interest.

In situations where there may be an apparent conflict of interest, and the conflicted-participant properly disclosed the potential conflict, bringing in an independent third-party can be an appropriate action. In advance of the actual transaction, this independent third-party could opine that the questioned transaction fairly represents a fair-market transaction.

EXAMPLE

The CEO owns real estate consisting of land and a building that is leased to the corporation in which the person is CEO.

A conflict of interest exists between the CEO's primary interest to maximize the corporation's profitability and the CEO's secondary personal interest to maximize their real estate investment return.

An independent third-party could evaluate the lease transaction to determine whether it complied with fair-market rates and terms.

Codes of Conduct that include ethics can minimize conflicts of interests by specifying potential conflicts and guiding appropriate behavior to avoid conflicts when faced with these conflicts. Further guidance addresses proper responses when faced with conflicts, such as refusing to proceed by removing themselves from the conflicting situation and appropriate internal disclosure.

Progressive organizations human resources department conduct educational programs that train employees on their Code of Conduct and conflicts of interest. Experience has shown that organizations can improve compliance and reduce risk through educating employees about acceptable and unacceptable behavior when they join the organization and having annual training to reinforce the Code of Conduct and conflicts of interest. The goal is for management and employees to recognize and defuse

This training includes how to recognize conflicts of interest and how this could lead to unethical decisions personally and lead to organization reputation risk. In addition, after training, an employee could not claim that they were unaware that there was a conflict of interest or that they were unaware their improper behavior was unethical.

EXAMPLE EMPLOYEE CODE OF CONDUCT

Employee Code of Conduct

As an employee, you are responsible to behave appropriately at work or on company business. We outline our behavioral expectations here in this Employee Code of Conduct document which you must read and sign annually. We can't cover every single case of conduct, but we expect that you will always use your best judgement and contact your supervisor or the Human Resources department for clarification before you act on uncertain issues any questions.

Table of Contents:

1. Dress code

2. Cyber security and digital devices

3. Internet usage

4. Cell phone

5. Corporate email

6. Privacy rights

7. Social media

8. Conflict of interest

9. Employee relationships

10. Employment of relatives

11. Workplace visitors

12. Solicitation and distribution

13. Disciplinary actions

14. Employee signature

1. Dress code

Our company's official dress code is business. Examples are slacks, mid-length dresses, loafers, collared shirts, and blouses. An employee's position, however, may also dictate how they should dress. If you frequently meet with clients or prospects, you should conform to a more formal dress code. We expect you to be clean when coming to work and avoid wearing clothes that are unprofessional such as shorts, t-shirts, and workout clothes.

As long as you conform to our guidelines above, we don't have specific expectations about what types of clothes or accessories you should wear.

We also respect and permit grooming styles, clothing, and accessories that are dictated by religious beliefs, ethnicity, or disability.

2. Cyber security and digital devices

This section deals with all things digital at work. Following are guidelines for using computers, phones, our internet connection, and social media to ensure security and protect our assets.

3. Internet usage

Our corporate internet connection is primarily for business. But, you can occasionally use our connection for personal purposes as long as they don't interfere with your job responsibilities. Also, we expect you to temporarily halt personal activities that slow down our internet connection (e.g. uploading photos) if you're asked to.

- You must not use our internet connection to:
- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and gain access to sensitive information.
- Download or upload pirated movies, music, material or software.
- Visit potentially dangerous websites that can compromise our network and computers safety.
- Perform unauthorized or illegal actions, such as hacking, fraud, or buying/selling illegal goods.

4. Cell phone

We allow use of personal cell phones at work. But, we also want to ensure that your devices won't distract you from your work or disrupt our workplace. We ask you to follow a few simple rules:

- Use your cell phone in a manner that benefits your work (business calls, productivity apps, calendars).
- Keep personal calls brief and use an empty meeting room or common area so as not to disturb your colleagues.
- Avoid playing games on your phone or texting excessively.

- Don’t use your phone for any reason while driving a company vehicle.
- Don’t use your phone to record confidential information.
- Don’t download or upload inappropriate, illegal or obscene material using our corporate internet connection.
- You must not use your phone in areas where cell phone use is explicitly prohibited (e.g. laboratories).

5. Corporate email

Email is essential to our work. You should use your company email primarily for work, but we allow some infrequent limited uses of your company email for personal reasons.

- Work-related use. You can use your corporate email for work-related purposes without limitations. For example, you can sign up for newsletters and online services that will help you in your job or professional growth.
- Personal use. You can use your email for personal reasons as long as you keep it safe, and avoid spamming and disclosing confidential information. For example, you can send emails to friends and family and download e-books, guides, and other safe content for your personal use.

No matter how you use your corporate email, we expect you to avoid:

- Signing up for illegal, unreliable, disreputable or suspect websites and services.
- Sending unauthorized marketing content or emails.
- Registering for a competitor’s services, unless authorized.
- Sending insulting or discriminatory messages and content.
- Spamming other people’s emails, including your coworkers.
- In general, use strong passwords and be vigilant in catching emails that carry malware or phishing attempts. If you are not sure that an email you received is safe, ask our information technology department.

6. Privacy rights

Employees have no legal expectation of privacy when using company resources, such as computers, networks, phones, or email. The company has the right to access, scan, or report on usage and content with any company electronic device.

7. Social media

We want to provide practical advice to prevent careless use of social media in our workplace. We address two types of social media uses: using personal social media at work and representing our company through social media.

Using personal social media at work. You are permitted to access your personal accounts at work. But, we expect you to act responsibly, according to our policies and ensure that you stay productive. Specifically, we ask you to:

- Discipline yourself. Avoid getting sidetracked by your social platforms.
- Ensure others know that your personal account or statements don’t represent our company. For example, use a disclaimer such as “opinions are my own.”
- Avoid sharing intellectual property (e.g. trademarks) or confidential information. Ask your manager or PR first before you share company news that’s not officially announced.

- Avoid any defamatory, offensive or derogatory content. You may violate our company's anti-harassment policy if you direct such content towards colleagues, clients or partners.

Representing our company through social media. If you handle our social media accounts or speak on our company's behalf, we expect you to protect our company's image and reputation. Specifically, you should:

- Be respectful, polite and patient.
- Avoid speaking on matters outside your field of expertise when possible.
- Follow our confidentiality and data protection policies and observe laws governing copyrights, trademarks, plagiarism and fair use.
- Coordinate with our [PR/Marketing department] when you're about to share any major-impact content.
- Avoid deleting or ignoring comments for no reason.
- Correct or remove any misleading or false content as quickly as possible.

8. Conflict of interest

When you are experiencing a conflict of interest, your personal goals are no longer aligned with your responsibilities towards the company. For example, owning stocks of one of our competitors is a conflict of interest.

In other cases, you may be faced with an ethical issue. For example, accepting a bribe may benefit you financially, but it is illegal and against our business code of ethics. If we become aware of such behavior, you will lose your job and may face legal trouble.

For this reason, conflicts of interest are a serious issue for all of us. We expect you to be vigilant to spot circumstances that create conflicts of interest, either to yourself or for your direct reports. Follow our policies and always act in our company's best interests. Whenever possible, do not let personal or financial interests get in the way of your job. If you are experiencing an ethical dilemma, talk to your manager or HR and we will try to help you resolve it.

9. Employee relationships

We want to ensure that relationships between employees are appropriate and harmonious. We outline our guidelines and we ask you to always behave professionally.

- Fraternization refers to dating or being friends with your colleagues. In this policy, "dating" equals consensual romantic relationships and sexual relations. Non-consensual relationships constitute sexual violence and we prohibit them explicitly.
- If you start dating a colleague, we expect you to maintain professionalism and keep personal discussions outside of our workplace.
- You are also obliged to respect your colleagues who date each other. We won't tolerate sexual jokes, malicious gossip and improper comments. If you witness this kind of behavior, please report it to the human resources department.
- Dating managers; to avoid accusations of favoritism, abuse of authority, and sexual harassment, supervisors must not date their direct reports. This restriction extends to every manager above an employee.
- If you act as a hiring manager, you aren't allowed to hire your partner to your team. You can refer them for employment to other teams or departments where you don't have any managerial or hiring authority.

- Employees who work together may naturally form friendships either in or outside of the workplace. We encourage this relationship between peers, as it can help you communicate and collaborate. But, we expect you to focus on your work and keep personal disputes outside of our workplace.

10. Employment of relatives

Everyone in our company should be hired, recognized or promoted because of their skills, character and work ethic. We would not like to see phenomena of nepotism, favoritism or conflicts of interest, so we will place some restrictions on hiring employees' relatives.

A "relative" is someone who is related by blood or marriage within the third degree to an employee. This includes: parents, grandparents, in-laws, spouses or domestic partners, children, grandchildren, siblings, uncles, aunts, nieces, nephews, step-parents, step-children and adopted children.

As an employee, you can refer your relatives to work with our company. Here are our only restrictions:

- You must not be involved in a supervisory/reporting relationship with a relative.
- You cannot be transferred, promoted or hired inside a reporting relationship with a relative.
- You cannot be part of a hiring committee, when your relative is interviewed for that position.
- If you become related to a manager or direct report after you both become employed by our company, we may have to transfer one of you.

11. Workplace visitors

If you want to invite a visitor to our offices, please ask for permission from our [HR Manager/ Security Officer/ Office Manager] first. Also, inform our [reception/ gate/ front-office] of your visitor's arrival. Visitors should sign in and show identification. They will receive passes and will be asked to return them to [reception/ gate/ front-office] once their visit is complete.

When you have office visitors, you also have responsibilities. You should:

- Always tend to your visitors (especially when they are underage).
- Keep your visitors away from areas where there are dangerous machines, chemicals, confidential records or sensitive equipment.
- Prevent your visitors from proselytizing your colleagues, gathering donations or requesting participation in activities while on our premises.
- Anyone who delivers orders, mail or packages for employees should remain at our building's reception or gate. If you are expecting a delivery, [front office employees/ security guards] will notify you so you may collect it.

12. Solicitation and distribution

Solicitation is any form of requesting money, support or participation for products, groups, organizations or causes which are unrelated to our company (e.g. religious proselytism, asking for petition signatures.) Distribution means disseminating literature or material for commercial or political purposes.

We don't allow solicitation and distribution by non-employees in our workplace. As an employee, you may solicit from your colleagues only when you want to:

- Ask colleagues to help organize events for another employee (e.g. adoption/birth of a child, promotion, retiring).
- Seek support for a cause, charity or fundraising event sponsored, funded, organized or authorized by our company.

- Invite colleagues to employee activities for an authorized non-business purpose (e.g. recreation, volunteering).
- Ask colleagues to participate in employment-related activities or groups protected by law (e.g. trade unions).
- In all cases, we ask that you do not disturb or distract colleagues from their work.

13. Disciplinary actions

Our company may have to take disciplinary action against employees who repeatedly or intentionally fail to follow our code of conduct. Disciplinary actions will vary depending on the violation.

Possible consequences include:

- Demotion
- Reprimand
- Suspension or termination for more serious offenses
- Detraction of benefits for a definite or indefinite time
- We may take legal action in cases of corruption, theft, embezzlement, or other unlawful behavior

14. Employee Signature

I assert that I have read and understood the employee Code of Conduct and that I have been in compliance for the twelve months from January, 20X0 to January, 20X1.

________________ ______

Employee Date

TONE AT THE TOP

An effective control environment has a strong influence on internal control effectiveness. The CEO has more impact than any other employee in setting the tone for ethical behavior, integrity, and internal control compliance. The CEO's actions establish the ethical environment for business behavior that influences how employees conduct themselves. If a conflict between control compliance and culture ever exists, culture will always win.

Company culture is established and communicated down from the top of an organization and reflects the organizations guiding values and ethical atmosphere. It is how things get done and what employees observe as behavior that get rewarded. Rewards are not just tangible monetary awards; they are often more frequent as perks such as office space and meeting seating, exposure to owners or higher-level executives, public praise, or favoritism in plumb assignments.

The "top" of any organization is the board of directors and the CEO. The board's approach and methodology of conducting its oversight responsibility first establishes the "Tone at the Top." The board has oversight authority over the entire organization and has the most direct impact through selecting the CEO.

The board hires the CEO, determines the CEO's continued employment status, and sets the CEO's compensation package. Following are criteria most boards consider in selecting a CEO. After selecting/retaining the CEO, the board's oversight responsibility includes monitoring and evaluating the CEO's performance according to many of these same factors.

- Leadership and motivational style
- Communication style
- Industry experience
- Professional network
- Functional experience
- Skills
- Ethical and moral character
- Shared values
- Strategic direction and major tactical approaches alignment with the board

The CEO is the organization's face and the person senior management, middle management, and other employees look up to for leadership, vision, motivation, and guidance. Effective CEO's build relationships and connecting with people within the organization as well as with external stakeholders. "Tone at the Top" comes from how transparently the CEO communicates their business, moral, and ethical values. The most obvious communication comes from written words and from oral presentations; however, the most influential communication comes from employees observing CEO behavior.

Just as the board measures the CEO's decisions, actions, and performance according to moral and ethical values, employees do the same. Unlike the board, however, employees use their observations to guide their own decisions and actions.

The CEO's ethical and moral tone will flow down to (and through) management and to all employees. If this tone exemplifies high ethics and morality, then management and employees are more likely to operate and behave with the same values. When the CEO and senior management communicate perfunctory ethical and moral values that become eclipsed by company profits or personal gain, employees will become more apt to behave similarly.

The right "Tone at the Top" is much more than controls and compliance systems. Too often, controls and compliance focus on avoiding legal issues instead of achieving strategic and operational business objectives. The right "Tone at the Top" develops organizational integrity by communicating the organization's guiding values so that they are understood and followed by management and employees. As a result, the entire organization conducts business and behaves according to ethical standards and the organizations values.

The right "Tone at the Top" is the best way to develop and maintain an organization's public reputation. It takes only one management or employee unethical gaffe to destroy a reputation.

Other advantages of the right "Tone at the Top" are that other organizations like to conduct business with other organizations that possess strong values and high ethical standards. This includes stakeholders and the entire supply chain from suppliers to customers as well as support functions. Furthermore, the right "Tone at the Top" will more likely attract the best employees and industry talent.

Setting the right "Tone at the Top" is properly communicating to employees that everyone from the CEO to part-time hourly employees are expected to follow high ethical standards and high integrity in conducting company business. Harvard Professor Lynn Paine outlined five critical factors to establishing an effective corporate ethics strategy.

1. Guiding values – must make sense and be clearly communicated to all organizational level so that all employees take responsibility for them. The CEO and senior management continuously reinforces company values through newsletters, posters, blogs, and employee meetings.

2. Personally committed leadership – the CEO and senior management must conduct business and exhibit actions consistently with company values and ethics. Actions speak louder than works which requires the CEO and senior management to visibly follow company values and ethics; otherwise, the rank-and-file employees will receive the message that these are merely lip service. Personal commitment establishes the right "Tone at the Top."

3. Support from other organization systems – other systems and structures must be consistent with the organization's values and ethics. The employee performance appraisal process needs to be sensitive to the means of achieving objectives and not the ends. The ends do not necessarily justify the means.

   One tool to accomplish this is a 360-degree evaluation process where a manager's performance rating is based on input from subordinates and peers as well as the traditional direct supervisor.

4. Integrate company values and ethics into everyday decision making. This includes strategic plans, budgets, marketing plans, supply chain dealings with suppliers and customers.

5. Empower managers to make ethically sound decisions. One approach is with ethics training. Web-based ethics training and customized Employee Code of Conduct training can improve recall through interactive scenario simulations. These simulations are of real-life situations managers are likely to face and can present practical advice on handling these situations. Web-based programs are generally multi-lingual which facilitates communicating a uniform message to global business with management in different countries.

EXAMPLE

Many companies have eagerly embraced collaborative technologies and the virtual workplace. Commuting drivers of this change are relatively-high gasoline prices, increasing car traffic congestion, increasingly unreliable and prohibitively expensive public transportation (especially New Jersey Transit or Metro North Railroad travel to Manhattan).

In addition, a virtual workplace is important to attracting, hiring, and retaining Millennials who highly-value a technology-enabled virtual workplace. Millennials covet greater flexibility to balance professional and personal lives. Disabled workers also benefit from a virtual workplace.

Finally, telecommuting or a virtual workplace originated in the progressive high-tech industry in the California Silicon Valley, where Yahoo! was founded and still remains, and is a well-established component of the high-technology industry culture.

In 2013 Marissa Mayer became the youngest woman to lead a major company when she was hired as CEO of Yahoo! This achievement, and because she was pregnant when she was interviewed and hired, made Marissa Mayer a visible role model to women and working mothers.

After being hired, Marissa Mayer squashed the telecommuting trend which reversed a long-standing Yahoo! policy. The CEO decided that employees could no longer work from home, even for one day if they had to wait for repair services or care for sick children. The Yahoo! policy change rationale was that working side-by-side improved communication and collaboration.

Yahoo! employees, both men and women, found the CEO's ban on telecommuting especially galling because the CEO brought her newborn to work and installed a nursery next to her office for the nanny and baby. This perk would not be available to other Yahoo! employees.

As a result of this Tone at the Top, company morale suffered. Yahoo! strategy went unfulfilled and operating and financial performance consistently missed targets.

In early 2017 after four years of continued declining operating and financial performance, Yahoo! was acquired by Verizon.

Key Techniques for Successfully Governing with a Dominant Visionary CEO

Strategic Finance, in September 2019, addressed the challenge for board members, investors, and employees figuring out how to deal with dominant visionaries who are often brilliant, unpredictable, difficult to work with, and sometimes downright mean. Middle and senior managers throughout the organization need to harmoniously survive and effectively deal with dominant, sometimes errant CEO visionaries.

Corporate governance principles and practices apply to all organizations, in all industries, organizations large and small, public and private, established or new start-up, closely held or widely dispersed. Appling core corporate governance principles and practices must be enhanced when there's a particularly strong leader.

Board members and those charged with governance can best support the creative talent of brilliant leaders (and often founders) while still maintaining the necessary structure, systems, internal controls, and guidance required for effective corporate governance. In other words, how can those charged with governance avoid getting in the way but ensure a rule-breaking CEO doesn't go haywire and do something weird, illegal, or stupid?

When dominant CEOs create toxic cultures, the costs to investors, employees, and other stakeholders can become enormous. The stock price can plummet, employees lose their jobs, suppliers get stiffed, and customer fulfillment gets disrupted. Examples are:

- **Volkswagen** – its CEO's lack of leadership gave rise to the company's tolerance for breaking the rules and cheating. The cost exceeded $20 billion.

- **Wells Fargo** – the CEO's improper sales practices and fraudulent activities with its customers resulted in fines exceeding $1.5 billion plus the cost of ongoing lawsuits.

- **Enron** – the CEO Ken Lay's illegal activities ruined the company, resulting in destroying $70 billion in shareholder value. Lay merged many companies in 1985 to become Enron, and under his leadership, Enron became the seventh largest U.S. company and Fortune magazine's most innovative company. Enron became the largest bankruptcy in U.S. history in 2001. Its downfall led to senior executives going to jail and other companies going out of business (including Arthur Andersen).

- **Theranos** – CEO Elizabeth Holmes thrilled investors with her vision to change healthcare but then was charged with multiple counts of fraud and conspiracy in federal court after investors lost nearly a billion dollars of their investment in her company (see "Costs of Maverick CEOs" for more examples). Holmes, a 19-year-old Stanford University dropout, was going to change the world with a new blood-testing system, but it never worked. She put together an all-star board of directors and a billion dollars of investor money. However, Holmes led Theranos to collapse and received many criminal charges for fraud and conspiracy for misleading investors, policy makers, and the public.

- **Uber** – CEO Travis Kalanick's vision changed the city transportation industry, but it also led him to be ousted from the company he founded. One exasperated Uber board member proposed adding "No brilliant jerks allowed" to Uber's list of cultural values. Kalanick founded Uber on breaking rules. His business model disrupted the highly regulated taxi business. He ignored regulations and plowed forward to great commercial successes. He was highly combative and controversial in both his company actions and personal behavior, leading to his being removed from leadership in 2017.

- **Apple** – CEO Steve Jobs was known as a visionary leader, but he also had a reputation for being a difficult, cantankerous jerk. Jobs founded Apple in 1976, was fired from the company in 1985, and rehired in 1997. He led the company to amazing growth until his death in 2011 and is regarded as one of the great dominant visionaries of all time.

- **Tesla** – CEO Elon Musk has behaved so erratically in the past few years that many have questioned his ability to lead. Musk has led the automobile company to tremendous growth, but he has also been at the forefront of controversy and confrontations with employees, government, competitors, media, and other stakeholders. He has a powerful vision for changing the world and shares it widely with overwhelming confidence, but many question if Tesla will succeed. Those betting on his failure have left Tesla one of the most shorted stocks in the world.

When a CEO's actions begin to damage the culture and long-term company success, the board can't permit a toxic culture or the leader's damaging actions to persist. At the same time, the board neither wants to kill the creativity and innovation that are the key to the rule breaker's success. Two important lessons emerged from dealing with the conundrum of a brilliant, but flawed, CEO.

- **An authoritarian trailblazer requires special handling.** The traditional corporate governance principles are needed, but they must be supplemented with additional practices. With an inspired and highly controlling powerhouse at the helm, boards, investors, and employees need to be ready for a different journey.
- **The best actions to govern, thrive, and survive depend on the type of CEO visionary.** Dominant visionaries aren't all the same. With some, there's a risk of getting in the way and curtailing the value they could create. With other types, complacency is a huge mistake, and, left unsupervised, their behavior could destroy the company.

According to Strategic Finance executive omniscience results from leaders creating a view that they have all the answers and that the board, investors, and employees should just follow their lead. There are three ingredients used by dominant visionaries to control their companies.

- Asymmetrical power. Dominant visionaries often have almost total control over their boards. Boards are supposed to be independent, but in many instances the CEO is also chairman and able to direct the outcome of all votes. In addition, dual-class ownership structures may provide the leader with absolute voting control.

  There exists a long history where corporate founders established multiple classes of stock so that unequal voting rights permit the founder to maintain corporate control through dual-class shares established to keep family control while bringing in public shareholders. Examples are Dodge Brothers' IPO in 1925 and Ford's IPO in 1956.

  More recently dual-class ownership became increasingly popular with Google's dual-class listing in 2004, followed by Facebook, Groupon, LinkedIn, and others. Founders often have voting rights of 10 times or more what the public shareholders have. Snap made dual-class share history by being the first company that issued nonvoting shares in its IPO.

  Dual-class shares give founders control so they can resist undue shareholder pressure and pursue their vision. The downside is it gives the founders disproportionate control and takes power from shareholders. To protect the long-term interests of the company, some companies establish over time an end date through sunset provisions that phase out the unequal voting control over five to ten years and restore a "one share, one vote" structure.
- Cult of personality. Many of these leaders are visionaries with bigger-than-life personalities coupled with a compelling story of their unique potential to change an industry and maybe the world. They are quite persuasive and able to convince people to follow them. These leaders exude confidence in pursuit of their vision and may bully people to fall in line.

- Lack of transparency. By controlling the free flow of information, leaders are often able to block visibility to performance data that is critical to effective decision making and governance. When the board isn't provided with essential information and is shielded from a clear picture of company performance, governance is significantly harmed.

The presence of any of these three ingredients doesn't guarantee that there will be a problem. There are many companies that have had overwhelming success with one, two, or all three of these. Their presence, however, signals there could be a problem. Thus, with dominant visionaries, additional board actions are often needed beyond its core roles and responsibilities:

- **Senior-level staffing and evaluation** – succession planning, compensation, and performance evaluations of senior executives.

- **Strategic oversight** – overseeing both strategy formulation and implementation.

- **Accountability** – governance practices, corporate behavior and ethics, and financial reporting and disclosure and internal control.

Boards must develop additional practices to deal effectively with a dominant visionary and their control over the information flow. Board members must become more active and control the agenda rather than permitting the CEO to take that role. Boards must focus carefully on both board composition and processes and they must be sufficiently strong and independent to ask the tough questions while facilitating collaboration and discussion.

Confronting a dominant visionary needs to be done with care because they often don't want to listen to contrary opinions. In addition, they often don't want to receive the oversight that boards of directors are supposed to provide—and don't want to listen to suggestions from their senior and middle-level managers. Being confronted in a board meeting or executive session often results in a defensive reaction. And sometimes the CEO's responses are downright nasty. Often, a one-on-one conversation outside of the boardroom or executive meeting is the right way to get things done.

The goal isn't to weaponize the board and constantly constrain the CEO. That could squash the value creation the brainy maverick is expected to bring. The role of the board, executive team, and investors is to support the disrupter-in-chief and provide just enough engagement and guidance to keep things from going wrong. Too much interference can destroy value; too little can destroy the company.

All senior and middle-level managers have a responsibility to report actions and behaviors that are potentially damaging to the company's future, and all employees have a responsibility to report ethical and legal violations.

CFOs and other financial executives are critical to effective governance practices. They have special responsibilities because of their roles in disclosure, internal control, accountability, and corporate governance.

The company must establish avenues for the safe reporting of any abuses, which can be difficult when the bad behavior is by the CEO. Without such reporting, however, senior leaders and the board of directors may be ignorant of the abuses.

AN EFFECTIVE WHISTLEBLOWING ENVIRONMENT

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) mandates that all public companies implement whistleblower programs. Because whistleblowing programs are highly-effective in discouraging and detecting wrongdoing, they also benefit non-public organizations.

In 1970, Ralph Nader, then best known as the author of "Unsafe at Any Speed," coined the term "whistleblower." He introduced this term to blunt unflattering terms often used to refer to someone that reported wrongdoing such as snitch, rat, fink, narc, or informer. Nader based his new term on the whistle that sports referees that blow when they see a rules infraction.

An effective whistleblowing environment depends on three factors: the organization's whistleblowing policies and procedures, the whistleblower who observes wrongdoing, and the organization-appointed person that receives the whistleblower report.

Whistleblowers often are not experienced reporters of any type of information, such as financial reports, book reports, media articles, or wrongdoing. Thus, an organization's whistleblowing policies and procedures cannot be written for the same audience as other controls, such as Sarbanes-Oxley compliance or auditors. Instead, the whistleblowing policies and procedures need to be written at a neophyte level of someone who may need direction recognizing wrongdoing, getting comfortable reporting wrongdoing, as well as the actual reporting methodology itself. Unfortunately, too many organizations whistleblowing policies and procedures address only the latter.

There are three destinations for reporting wrongdoing.

1. **Internal** – the most common type of reporting wrongdoing where an employee observing and reporting organization wrongdoing follows their organization's internal procedures. Internal destinations may not allow employees to report anonymously and without fear of retaliation. As a result, employees that suspect wrongdoing either may not report it or may choose to report external to the organization.

2. **Internal-appointed third-party** – this is typical for organizations that designate through their internal policies an external third-party to receive employee reports of wrongdoing. This destination developed to encourage employees to report suspected wrongdoing internally instead of automatically turning to an external destination.

   The goal is to minimize employee's concerns of retaliation because their report goes to an outside organization who then contacts the employer organization about the report while maintaining the employee's confidentiality. An additional advantage of this destination is that it would not violate any Non-Disclosure Agreement the employee may have been required to sign as a consideration of employment.

3. **External** – where an employee observing and reporting wrongdoing contacts parties outside their employer. Examples of external parties are government regulators, law enforcement agencies, personal lawyers, or news media.

Many organizations have two levels of reporting wrongdoing, a complaint process and a whistleblower process. The dual levels often exist because employees may confuse the difference between lesser-issue conflicts, which are not illegal, with greater-issue illegal fraudulent acts.

The organization's goal is to encourage employees to come forward with concerns and to funnel minor infractions through the complaint process instead of through a higher-involved full fraud investigation. A complaint process, however, must not replace a formal whistleblowing process. A complaint process is inadequate to handle true unethical business practices or illegal wrongdoing, and it is strictly an internal process which does not protect the reporting-employee with anonymity nor confidentiality.

An internal-appointed third-party whistleblower process, often referred to as a "whistleblower hotline" should contain the following attributes:

- Be accessible 24/7 for 365 days per year. This allows employees to file a report from a location other than the organization which offers employees two advantages. First, it increases the likelihood of remaining anonymous because the report filing is completed outside the organization. Second, an evening or weekend report filing may allow the employee to feel more relaxed which can clarify their thinking.

- Be broadly accessible by stakeholders. Beyond employees, suppliers and customers may also learn of wrongdoing and should have reporting access. In addition, supplier anonymity is especially important for stakeholder suppliers that may fear loss of business if it became known that they filed a report.

- Have multiple contact points. Examples are toll-free phone number, toll-free fax number, regular mail address, e-mail address, and on-line forms.

- Be broadly communicated. Examples are posters placed conspicuously in organizations locations such as the lobby, cafeterias, and wash rooms; posted on the organization website; listed in employee handbooks; and available alongside other organization information given to employees such as employee benefits.

Employee education and training, typically conducted by or arranged through the Human Resources department is important. This applies both to new hire orientation and to annual reinforcement training for existing employees. Furthermore, this training also teaches organization culture and standards for conducting business and appropriate employee behavior.

The training benefits are beyond how to use the process in filing a report, how anonymity is protected, and how a reporter will be supported post-filing. Most importantly, training provides education about how to recognize wrongdoing and shows how wrongdoing harms the organization.

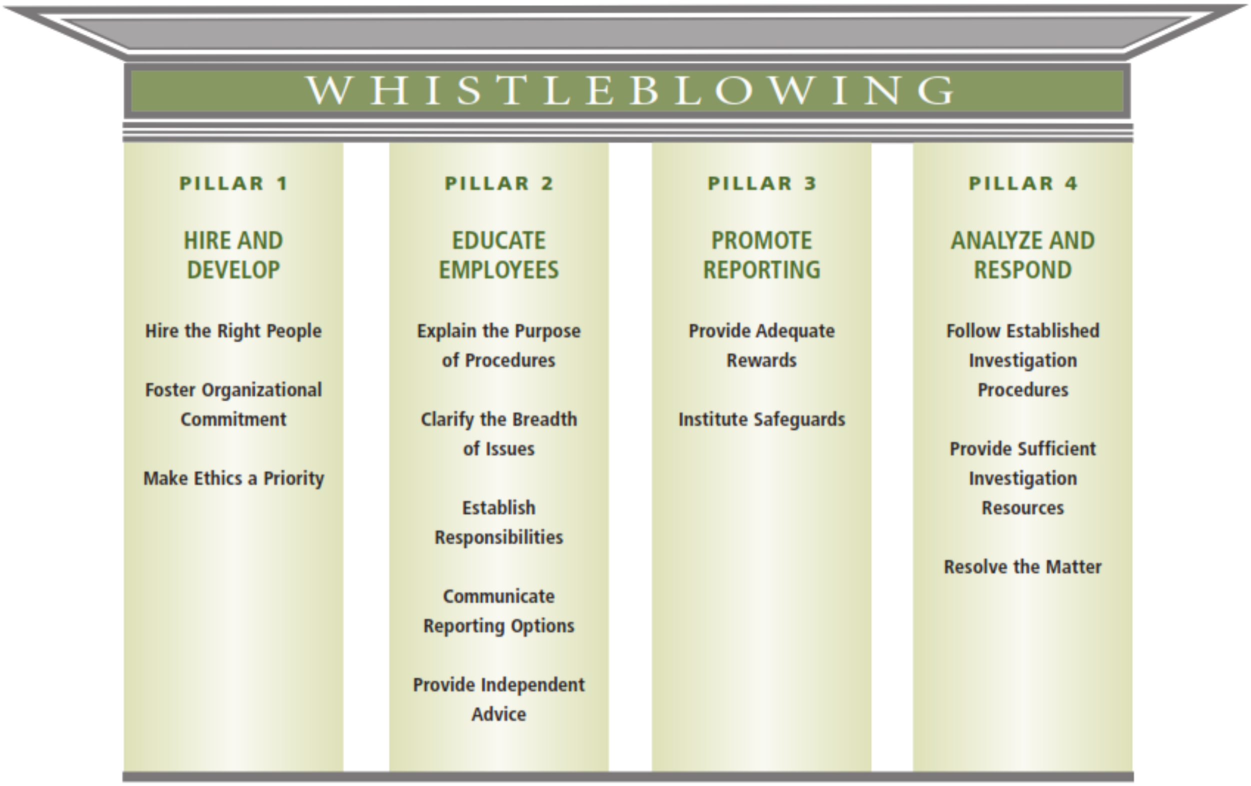
All controls require regular monitoring for design effectiveness, implementation, and operational effectiveness. For a whistleblower process, additional monitoring covering the number of reports, type of wrongdoing reported, and outcome of the investigation are also important. This report analysis may indicate control weaknesses and cultural shortcomings that may need to be addressed by additional employee training and education.

A low number of wrongdoing reports may not necessarily indicate a high level of control compliance, ethical workforce, desired culture, or lack of wrongdoing. It also may indicate a control design deficiency or employee hesitancy to file a report after they witnessed wrongdoing.

A high number of wrongdoing reports may indicate something different than improper employee behavior and unethical business dealing. This is because some whistleblower programs may create an unfavorable employee incentive to chase monetary rewards or to act like spies or law enforcement officials.

The Four Pillars of an Effective Whistleblowing Environment – *Strategic Finance, March 2014*

In March 2014, Strategic Finance published *Creating an Effective Whistleblowing Environment.* [13] This article identified four pillars of a successful whistleblowing environment, which is shown below.


WHISTLEBLOWING

PILLAR 1

HIRE AND DEVELOP

Hire the Right People

Foster Organizational Commitment

Make Ethics a Priority

PILLAR 2

EDUCATE EMPLOYEES

Explain the Purpose of Procedures

Clarify the Breadth of Issues

Establish Responsibilities

Communicate Reporting Options

Provide Independent Advice

PILLAR 3

PROMOTE REPORTING

Provide Adequate Rewards

Institute Safeguards

PILLAR 4

ANALYZE AND RESPOND

Follow Established Investigation Procedures

Provide Sufficient Investigation Resources

Resolve the Matter

1. Hire and develop potential whistleblowers

   An effective whistleblowing environment begins with employees that are comfortable reporting wrongdoing that they witness. Thus **during the hiring process**, it is important to determine a job candidate's personal characteristics that indicate someone more likely to report wrongdoing. These personal characteristics are:

[13] https://sfmagazine.com/wp-content/uploads/sfarchive/2014/03/Creating-an-Effective-Whistleblowing-Environment.pdf

- Greater awareness of the opportunities for wrongdoing in their organizations
- Stronger connection to the organization
- A stronger professional identity
- A stronger moral character relative to non-whistleblowers

One indicator of these personal characteristics is belonging to and professional organization because many organizations require ethical values as a condition of membership. The organization should encourage and support existing employees, for this same reason, to become active in their professional organizations. If the position has direct influence over financial reporting, discuss the job candidate's ethical beliefs and under what circumstances they would consider blowing the whistle.

Organizations can **foster an organizational commitment** by creating and maintaining a culture that nurtures loyalty. Organizations accomplish this in several ways. First, provide organization-branded clothing and logoed office supplies which are effective at creating organizational identification. Second, establish compensation that is both equitable within the organization and comparable to peer-organizations. Third, maintain a high level of organizational justice by resolving conflicts equitably, conducting fair and transparent annual performance reviews, and ensuring that organization policies are followed judiciously.

Organizations can **make ethics a priority** by making it clear that employees are expected to act with integrity and by defining integrity. Organizations accomplish this in several ways. First, conduct employee training that outlines management's ethical expectations while instilling employee confidence required to make tough ethical decisions. Second, by setting a "Tone at the Top" marked by high ethical standards, demonstrating decision making integrity, and publicly praising ethical actions while privately correcting unethical choices.

2. Educate employees

Employee education is not only for new-employee orientation but also should be provided periodically for all employees. Whistleblowers can report wrongdoing only when they understand: how to recognize wrongdoing, their responsibility to report it, and how to report it properly. Organizations can take several steps to train their employees about whistleblowing.

Organizations need to **explain the whistleblowing procedure purpose** so employees understand why the organization needs a whistleblowing program. This is similar to why a private company chooses to pay for an external financial audit because it provides greater evidence that management and its financial reports are trustworthy. Accordingly, proper employee whistleblowing training can increase the trust level within the organization in at least two ways. First, those in a position to blow the whistle will have greater reason to trust that they will be protected from reprisals for whistleblowing. Second, employees will have greater trust that they won't be punished for baseless charges.

Education should ease employee concerns that they work in an environment in which their peers are watching their every move in order to detect wrongdoing, which can lead to an environment of paranoia and distrust. Instead, employees can understand that whistleblowers are ethical people who acted on their obligation to report wrongdoing they observed during the normal course of business; and not that they went out of their way searching for evidence of wrongdoing.

Training **clarifies the breadth of whistleblowing issues** by communicating types of conduct that do and do not warrant whistleblowing. Defining the spectrum of issues can increase attentiveness to wrongdoing.

EXAMPLES

While there's no question that employees who accept kickbacks from suppliers should be reported, many employees may wonder if they need to report a coworker who accepts small gifts or a lunch from a supplier.

An employee who leaves work early for a personal lunch likely doesn't warrant reporting, but one who expenses his personal lunch probably does.

A supervisor who dismisses a single study that suggests a minor safety problem with a product likely doesn't need to be reported, but one who ignores the serious negative implications of several studies may warrant blowing the whistle.

Failure to remind employees about the types of issues that should be reported can be seen in the case of Treasurer David Myers at WorldCom.

EXAMPLE

David Myers was an experienced accountant who joined WorldCom in 1995 as treasurer. When Myers presented quarterly financial statements in 1999 that failed to meet analysts' forecasts, his boss, WorldCom CFO Scott Sullivan, instructed him to find his "mistake."

After redoing and presenting similar financials, Myers was again told to find his mistake. Ultimately, WorldCom released accounting reserves to close the difference between what Myers was reporting and what CFO Sullivan thought the numbers needed to be.

Instead of blowing the whistle, Myers remained silent. His alleged "error" was never found, and WorldCom repeated again and again the accounting reserve release to "correct" other errors. Myers believed he had to protect the jobs of WorldCom employees by allowing these unethical accounting treatments. What began as a seemingly simple accounting adjustment escalated into one of the largest frauds in business history?

Organizations need to **establish whistleblowing responsibilities** so employees know that everyone is obligated to blow the whistle and will face consequences for failing to report a wrongful act. For example, if an employee observes a wrongful act and doesn't report it, will that person be terminated or face lesser penalties? If there are no consequences, that employee may question whether there truly is a responsibility to report wrongdoing.

Periodically highlighting whistleblowing importance reinforces employee's wrongdoing reporting responsibilities. For example, management can share news stories by e-mail or in company-wide training about cases in which unreported fraud led to organizational failure or where reported fraud led to organizational success. In the unfortunate event that an observed fraud occurs in the organization that the observing-employee does not report, the disciplinary action taken against that employee for remaining silent should be communicated to all employees to discourage others from turning a blind eye.

A whistleblower has the responsibility is to provide a truthful report. As a result, the whistleblowing policy must contain a "good-faith" requirement that protects employees from false accusations as well as avoids spending organizational resources investigating false leads. If an employee knowingly provides a false report, then appropriate disciplinary action should be taken.

Organizations need to **communicate whistleblower reporting options**. Employees must be taught how to communicate their wrongdoing concerns appropriately. Specifically, it's essential that employees understand to whom they should contact about any wrongdoing concerns. Reporting to the wrong individual may not trigger an appropriate investigation, and the whistleblower may not be protected from retribution.

Larger organizations should consider whether a tiered reporting system is appropriate. For example, in an initial tier, employees can raise concerns to their immediate supervisor. This informal communication may facilitate a more expedient investigation. A second tier could involve reporting concerns to upper management or the board of directors, which could trigger a more formal investigation. A final tier is outside reporting. Although it isn't necessarily optimal, employees should be aware of the option to report to regulators such as the Internal Revenue Service (IRS) or U.S. Securities & Exchange Commission (SEC). The Institute of Management Accountants (IMA) Statement of Ethical Professional Practice explicitly provides a detailed example of tiered procedures for the resolution of ethical conflict.

Training also indicates how employees should communicate their wrongdoing concerns, such as face-to-face, whistleblowing hotlines, an Internet site, or paper comment boxes. To ensure internal employee confidentiality, many organizations outsource this process. However, complete confidentiality protecting the whistleblower's identity even to an external recipient creates a dilemma. Confidential reporting is advantageous because it may lessen the social cost of reporting; however, it also may create an environment in which employees and their supervisors need to deceive others to protect confidentiality. Furthermore, maintaining confidentiality actually may hinder a wrongdoing investigation by reducing transparency. Each organization must determine the process that works best for its own program and communicate that to employees.

Organizations should **provide awareness of independent advice** to employees because this reduces the risk that a whistleblowing procedure misunderstanding could result in a fraud going unreported. One solution is for an organization to provide access to a legal-advice hotline that may contact if they are uncertain if something warrants reporting or if they're nervous about bringing it to a superior without support. In many cases, a potential wrongdoing reporting decision may be blurred by ambiguous statements.

EXAMPLE

A supervisor who instructs the bookkeeper to record an inappropriate transaction is clearly wrongdoing that needs to be reported. However, if a supervisor asks the bookkeeper to use an aggressive estimate or to "find a way," this request may not warrant reporting. In this setting, an independent advisor can provide guidance and potentially avoid a formal investigation.

3. Promote wrongdoing reporting

   After assessing the evidence, the prospective whistleblower must decide whether to report the wrongful act. To promote reporting, an organization should provide rewards and safeguards to whistleblowers. If an employer does not protect a whistleblower, ethical violations and fraud will not be reported.

   Organizations need to **provide adequate rewards** for reporting wrongdoing because whistleblowers frequently incur significant social costs for reporting on their peers. Any reward needs to be clearly specified how rewards are determined, including the context and conditions that qualify for reward. For example, the reward can be a fixed amount or a percentage of the size of fraud uncovered. The conditions that need to be met to merit a reward may include wrongdoer criminal prosecution, criminal conviction, or simply an organizational finding that wrongdoing occurred.

   Organizations need to **institute safeguards** that provide adequate protection of whistle- blowers so that employees aren't deterred by fear of reprisal. The most common safeguard is assurance that the whistleblower won't be fired. Other safeguards could be transferring the employee to another business unit at the same level, an extended paid leave for training to transfer to a new position, or an appropriate separation package if the employee finds the working environment to be hostile after blowing the whistle. Several laws at the federal and state levels protect whistleblowers from retaliatory acts, including termination.

   These safeguards also need to extend to protect employees from false accusations. Such protection may involve working with labor unions and other stakeholders to assure that all employees' rights are protected. Also, policies should specify requirements for corroboration of accusations and provide a protocol for bringing in outside assistance for accused employees when such assistance is requested.

4. Analyze and respond appropriately to all whistleblowing reports

   The whistleblowing process effectiveness depends on an appropriate analysis and response by those who receive the whistleblower report. The process requires both formal procedures and adequate resources to ensure that every claim is addressed appropriately.

   Organizations need to establish and **follow established investigation procedures** about how to respond to a whistleblower report. Auditors, audit committee members, or Certified Fraud Examiners (CFEs) can be useful resources to help develop these procedures. Organizations need to specify the investigation team responsibilities, such as documenting the whistleblower accusation, deciding whether to investigate, conducting the investigation, and recommending the appropriate response.

The investigation team needs proper training on investigative procedures. This training may consist of investigators attending workshops or webinars hosted by professional associations, or periodically bring in an expert to train managers, internal auditors, and board members.

Organizations need to **provide sufficient investigation resources** to conduct the whistleblower investigation and pay any reward to the whistleblower. Investigators need access to internal audit, relevant department heads, and others to collect evidence. They also may need to hire outside legal counsel, CFEs, or other specialists to help investigate the report.

Once the investigation concludes, the organization needs to **resolve the matter**. Resolution can range from terminating the accused to taking no action against them. Resolution includes communicating the investigation conclusions to both the accused and the whistleblower and verifying that the investigation followed all specified whistleblowing procedures. This verification is important even when the investigators conclude to take no action because there is a significant difference between (1) concluding there was insufficient evidence to take action, versus (2) finding sufficient evidence that proved nothing wrong occurred.

Finally, the investigation team must document all reports and responses. These records may play a vital role in future investigations and can serve as a deterrent against future wrongdoing. In addition, the team should remove names from the records to protect individuals who were falsely accused.

In conclusion, whistleblowing isn't just a program. It is an organization cultural mind-set that holds employees accountable for their actions and makes everyone in the organization responsible for reporting wrongdoing. This mind-set begins by hiring employees who will carry out their whistleblowing responsibilities, and it's reinforced through education and visible management action. The whistleblowing mind-set compels employees to report any wrongdoing they see and assures that all reports are resolved appropriately.

Talking about ethics is useless if employees do not witness management visibly demonstrating its commitment to integrity and ethics. This commitment requires management to walk the walk in addition to talk the talk.

Employees must believe that their employer values ethical violation reporting, and the best way for organizations to accomplish this is through regular communication and training, plus reinforcement through management actions. When there is a whistleblower report filed:

- It must be thoroughly investigated
- Violators need to be punished according to published policy
- If the investigation conclusion is no action, this and the reasons need to be communicated back to the person who filed the whistleblower report

- Internal controls that failed to prevent or detect the wrongdoing need to be analyzed and improved

Whistleblowing requires constant monitoring so the procedures do not become outdated or forgotten. Every organization is susceptible to fraud; thus, every organization needs to monitor its control environment to minimize the risk of unreported wrongdoing.

EXAMPLE CONTROLS

Following are examples of approaches that small to mid-size entities can use to implement controls at the control environment, along with documentation that they should consider to evidence that control's implementation. Adequate documentation makes it easier for the auditor to perform risk assessment procedures. When the entity does not provide adequate documentary evidence, the auditor is challenged to accomplish the observation and inspection.

Note that the examples listed below are options for the entity. Not every entity will implement every control.

EXAMPLE APPROACHES THAT SMALL TO MID-SIZE ENTITIES CAN USE

Principle 1. The organization demonstrates a commitment to integrity and ethical values.

- A process exists by which those charged with governance are made aware of key developments that may affect financial reporting.
- Management, employees, and others are made familiar with the entity's policies and practices with regard to ethics, accepted operating practices, and positive control environment.
- Management acts to remove or reduce incentives or temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts.
- The organization has adopted and communicated to employees and board members, donors, volunteers, and vendors a specific policy on conflict of interest that specifies that personnel in a position of trust are not related to each other; employees are prohibited from having business dealings with companies affiliated with, or who act as major customers or suppliers of, the organization; transactions with officials of the organization are adequately controlled and disclosed in the records; and such transactions occur only in the normal course of business and are approved by the governing board.
- Rewards, such as merit pay and other incentives, foster an appropriate ethical tone.
- Management sets realistic financial targets and expectations.
- Management follows ethical guidelines in dealing with external audiences, including suppliers, contributors, creditors, insurers, etc.
- Relationships with professional third parties are periodically reviewed to ensure the entity maintains association with reputable parties.
- "Risk appetite," or amount of risk the entity is willing to accept, associated with each new venture is discussed and influenced by the entity's culture and operating practices.

- Management exemplifies attitudes and actions in line with its mission, vision, and values to support an effective control environment.
- Management gives appropriate attention to internal controls and corrects any known weaknesses in internal controls on a timely basis.
- Management regards the accounting function as a means for monitoring and exercising control over the entity's various activities.
- Management adopts accounting policies that are appropriate for the entity and consistent with GAAP (or an OCBOA).
- Management sets the tone that high-quality and transparent financial reporting is expected.
- Management establishes human resources policies and procedures that demonstrate its commitment to integrity, ethical behavior, and competence.
- Employee recruitment and retention practices for key financial positions are guided by principles of integrity and by the necessary competencies associated with the positions.
- There are formal policies and procedures to evaluate employee performance and compensation.
- Job performance and competencies are periodically evaluated and reviewed with each employee.

Principle 2: The governing board demonstrates independence from management in exercising oversight of the development and performance of internal control over financial reporting.

- The makeup and general construction of the governing board and its committees are appropriate and adequate given the nature of the entity.
- Those charged with governance are sufficiently involved with the entity to address important oversight responsibilities.
- Those charged with governance provide input and oversight of the entity's financial statements, including the application of GAAP (or an OCBOA) and use of accounting judgments.
- A process exists by which those charged with governance are made aware of key developments that may affect financial reporting.
- The governing board is sufficiently independent of management so that necessary questions are raised.

Principle 3: With board oversight, management establishes structures, reporting lines, and appropriate authorities and responsibilities to achieve financial reporting objectives.

- The organizational structure is commensurate with the entity's activities.
- Management periodically evaluates the entity's organizational structure and makes necessary changes based on changes in its activities and/or industry.
- The entity defines key areas of authority and responsibility, including management's responsibility for entity activities, and how they affect the entity as a whole.
- There is a structure for assigning ownership of data, including who is authorized to make and/or modify transactions.
- There are policies for offering new services, conflicts of interest, and security practices that are adequately communicated to all employees in the organization.
- A process exists to support the identification and disclosure of related party relationships and transactions.

Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with financial reporting objectives.

- Management establishes human resources policies and procedures that demonstrate its commitment to integrity, ethical behavior, and competence.
- Human resources policies and procedures are clearly communicated to employees and issued, updated, and revised on a timely basis.
- Employee recruitment and retention practices for key financial positions are guided by principles of integrity and by the necessary competencies associated with the positions.
- There are formal procedures for the hiring (recruiting) and retention of employees.
- There are formal policies and procedures to evaluate employee performance and compensation.
- Job descriptions, reference manuals, or other forms of communication inform personnel of their duties.
- The entity establishes competencies (knowledge, skills, abilities, and credentials) prior to hiring of key positions.
- Employees tend to have the competence and training necessary for their assigned level of responsibility or the nature and complexity of the entity's activities.
- Job performance and competencies are periodically evaluated and reviewed with each employee.
- All departments are appropriately staffed.
- Management demonstrates a commitment to provide sufficient accounting and financial personnel to keep pace with the growth and/or complexity of the entity's activities.

Principle 5: The entity holds individuals accountable for their internal control responsibilities.

- A code of conduct or ethics policy exists.
- Management, employees, and others are made familiar with the entity's policies and practices with regard to ethics, accepted operating practices, and positive control environment.
- Management acts to remove or reduce incentives or temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts.
- Rewards, such as merit pay and other incentives, foster an appropriate ethical tone.
- Management sets realistic financial targets and expectations.
- There are formal policies and procedures to evaluate employee performance and compensation.
- Employees are empowered to correct problems or implement improvements in their assigned processes.
- Job performance and competencies are periodically evaluated and reviewed with each employee.

Unit

6

Risk Assessment

LEARNING OBJECTIVES

After completing this unit, participants will be able to:

□ Assess risk

□ Apply COSO risk assessment approaches

□ Identify, detect, and prevent fraud

□ Understand the impacts of the human element of fraud

Audit Standard No. 5, *An Audit of Internal Control over Financial Reporting That Is Integrated with An Audit of Financial Statements*, addresses risk assessment. Organizations can benefit from audit guidance which provides relevant direction beyond auditing. AS-5 paragraph 10 states:

> Risk assessment underlies the entire audit process described by this standard, including the determination of significant accounts and disclosures and relevant assertions, the selection of controls to test, and the determination of the evidence necessary for a given control.

Risk can be broadly defined, and it applies to achieving business objectives and financial reporting objectives. As it applies to financial reporting, risk is when the lack of controls or the controls implemented "**could**" allow a material misstatement in the financial statements. Financial reporting risk also applies to not disclosing a material fact.

"Could" is an important distinction because a risk need only have the potential to lead to a material misstatement. There does not have to be an actual bad occurrence for a risk to be identified.

EXAMPLE

An organization prepares its financial statements in compliance with GAAP. Financial reporting risks would be potential impediments to achieving this financial reporting objective. These risks could include management judgment, calculation errors, errors due to GAAP complexity, asset existence, valuation, disclosures, and more.

An example of how operational control failures can impact financial reporting, such as entity valuation, asset valuation, potential impairment, is Chipotle. Chipotle's 2015 food poisoning outbreak destroyed the "darling of fast food's" reputation and equity valuation.

EXAMPLE

Chipotle, in 2015 had reported strong revenue growth for almost a decade. In December 2015, however, Chipotle warned that it expects significant declines at its flagship stores as a result of its food contamination outbreak. Chipotle's stock price, fell by nearly 30% since its food contamination outbreak was first detected.

Chipotle became the darling of the fast-food world by attracting millennials, blue-collar workers, and even whole families with its promise of high-quality, sustainably-sourced, Mexican-inspired cuisine. Chipotle's pledge of higher-quality food is prominent on its website, where it trumpets the core mission of "food with integrity" and emphasizes a respect for animals, farmers, customers and the environment.

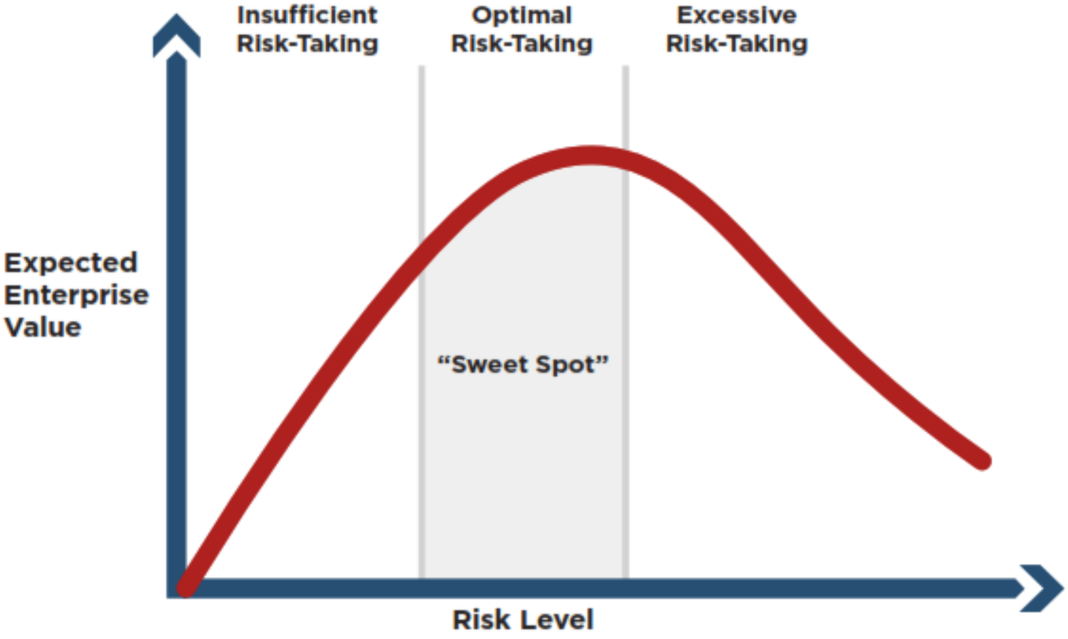
But a series of food poisonings and other challenges destroyed Chipotle's reputation. Chipotle's reputation is perhaps more at risk than most in the fast-food industry because the chain has promised that it adheres to more-rigorous standards for procuring and serving its food. Now, industry experts warn it could face a permanent red mark even if the latest spate of setbacks proves temporary.

Management decisions increase, preserve, or erode organization value. Thus, risk assessment is important because risk and return determine value. Risk assessment is identifying risks and then evaluating how significant each risk is to the organization achieving its goals.

Management strives to manage risk exposures across the organization according to the board of director's risk appetite so that management optimizes risk to pursue strategic objectives and achieve their expected enterprise value goals. An optimal risk-management graph from COSO is shown on the next page. The 'sweet spot' is the optimal risk level based on the board's risk appetite.[14]

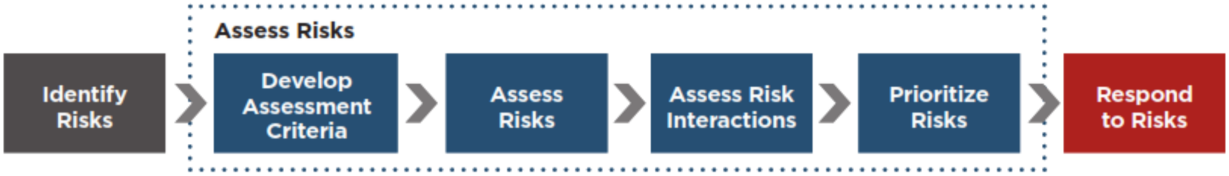
To optimize value, organizations conduct a risk assessment process, which must be practical, sustainable, and proceed in a structured and disciplined fashion. Management's risk assessment needs to be properly structured for the organization's industry, size, complexity, and geographic presence. This process is also called Enterprise Risk Management (ERM).

Within the COSO ERM framework, risk assessment begins with risk identification and ends with risk response. The ERM process involves assessing the magnitude of identified risks, both individually and in the aggregate. This, in turn, directs management's attention to the most important risks within the board's communicated risk appetite. Management then prioritizes the identified risks and develops risk responses. Management aims to manage risks by not becoming over-controlled and therefore forgoing desirable opportunities.



Some risks are dynamic and require continual ongoing monitoring and assessment, such as certain market and production risks. Other risks are more static and require reassessment on a periodic basis with ongoing monitoring triggering an alert to reassess sooner should circumstances change.

Below is the COSO risk assessment flow diagram.14



The process begins with **risk identification** across the entire organization. The risk-identification output is a comprehensive risk list, which is then organized by:

- risk category – strategic, operational, financial, compliance
- sub-category – market, credit, liquidity
- organization – corporate, operating units, large capital projects

After identifying risks, management performs a **four-stage risk assessment** that ultimately results in risk prioritization. This risk prioritization focuses management on the most important risks. A secondary risk-identification benefit is identifying opportunities as well.

Develop Risk Assessment Criteria Standards

Following risk identification, management develops risk assessment criteria standards that apply to the entire organization. The most important measures commonly employed are impact and likelihood; however the four most common criteria examples are:

- impact size
- occurrence likelihood
- vulnerability
- onset velocity

To include unlikely events that, when they occur, seem to occur at lighting speed, we also include vulnerability and onset speed. These latter two criteria address organization response and recovery time as well as tolerance for operating down time. Vulnerability to a risk event helps define specific control needs, and onset velocity helps define agility needs.

When management rates risk impact, it needs to rate risk at the highest expected consequence. If a risk contains several risk criteria, and the highest criterion rating is a five, then that risk's total impact rating is a five.

Risk, or any for that matter, measurement requires a scale to interpret meaningfulness. A risk measurement scale is required not only for risk assessment but also for comparing and aggregating risks across the entire organization. Management needs to define the risk measurement scale so that the organization applies, rates, and assesses risk consistently. Scales also product meaningful differentiation for risk ranking and prioritization. Because every organization is different, risk measurement scales should be customized to the organization based on industry, size, complexity, geographical reach, and culture.

Scale measurement properties are:

- **Identity** – each value on the measurement scale has a unique meaning.
- **Magnitude** – values on the measurement scale have an ordered relationship to one another. That is, some values are larger and some are smaller.
- **Equal intervals** – scale units along the scale are equal to one another. For example, the difference between 1 and 2 would equal the difference between 19 and 20.

Five-point scales are generally best for risk measurement. Ten-point scales are generally too large because they may imply greater precision than truly exists. Also, risk measurers may spend unproductive time rating a risk between, for example 8 or 9, when this difference is not meaningful, inconsequential, or indefensible.

- **A minimum value of zero** – scale has a true zero point, below which no values exist.

Impact is the consequence of having the risk, and its measurement is the extent a risk event might affect the organization. Financial risks are not the only risks impacting an organization. Management defines impact using impact assessment criteria such as financial, reputational, regulatory, health and safety, security, environmental, employee, customer, and operations. Some risks impact the organization financially, while other risks may have a greater reputation, rather than, financial risk.

An example of a **risk impact scale** from COSO is shown below:

Rating	Descriptor	Definition
5	Extreme	Financial loss of $X million or more International long-term negative media coverage; game-changing loss of market share Significant prosecution and fines, litigation including class actions, incarceration of leadership Significant injuries or fatalities to employees or third parties, such as customers or vendors Multiple senior leaders leave
4	Major	Financial loss of $X million up to $X million National long-term negative media coverage; significant loss of market share Report to regulator requiring major project for corrective action Limited in-patient care required for employees or third parties, such as customers or vendors Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
3	Moderate	Financial loss of $X million up to $X million National short-term negative media coverage Report of breach to regulator with immediate correction to be implemented Out-patient medical treatment required for employees or third parties, such as customers or vendors Widespread staff morale problems and high turnover
2	Minor	Financial loss of $X million up to $X million Local reputational damage Reportable incident to regulator, no follow up

		No or minor injuries to employees or third parties, such as customers or vendors General staff morale problems and increase in turnover
1	Incidental	Financial loss up to $X million Local media attention quickly remedied Not reportable to regulator No injuries to employees or third parties, such as customers or vendors Isolated staff dissatisfaction[14]

Likelihood is the occurrence possibility that a specific risk event. It is generally expressed both in qualitative and in quantitative terms. Qualitative term examples are: frequent, likely, possible, unlikely, and rare. Qualitative terms may also include personal references, such as “an event expected to occur several times over the course of a career.”

Quantitative values are a percentage or frequency. When using quantitative numerical values, specify the relevant time period, such as annual frequency or relative probability over the project or asset life.

An example of a **risk likelihood scale** from COSO is shown below:

Rating	Annual Frequency		Probability	
	Descriptor	**Definition**	**Descriptor**	**Definition**
5	Frequent	Up to once in 2 years	Almost	90% of greater chance of occurrence over life of asset or project
4	Likely	Once in 2 years up to once in 25 years	Likely	65% up to 90% chance of occurrence over life of asset or project
3	Possible	Once in 25 years up to once in 50 years	Possible	35% up to 65% chance of occurrence over life of asset or project
2	Unlikely	Once in 50 years up to once in 100 years	Unlikely	10% up to 35% chance of occurrence over life of asset or project
1	Rare	Once in 100 years or less	Rare	<10% chance of occurrence over life[15]

[14] https://www.pace2race.com/lessons/risk-assessment-tools/

[15] https://www.pace2race.com/lessons/risk-assessment-tools/

Comparing impact size with occurrence likelihood can establish control prioritization. For example, a risk that is low in both impact size and occurrence likelihood would be have controls of lesser importance. As either impact size, or occurrence likelihood, or both increase, the controls for these risks increases in importance.

Vulnerability is related to both impact and likelihood. It is the organization's susceptibility to a risk event based on the organization's preparedness, agility, and adaptability. Greater vulnerability indicates a higher impact should the risk event occur.

Assessing vulnerability gauges how well management is managing risks. For example, if controls are not implemented, have a design deficiency, or are not operating as designed, then the likelihood of a risk event occurring increases.

Vulnerability assessment criteria include organizational capabilities to anticipate events. Examples are scenario planning, real-asset options (planned excess capacity for strategic opportunity), implemented preventative risk responses, capabilities to respond or adopt quickly as risk events evolve, and capabilities to withstand the risk event itself (financial strength of liquidity and solvency; capital buffer of excess borrowing capacity). External factor criteria examples would be industry change rate or organization change rate.

An example of a **risk vulnerability scale** from COSO is shown below:

Rating	Descriptor	Definition
5	Very High	No scenario planning performed Lack of enterprise level/process level capabilities to address risks Responses not implemented No contingency or crisis management plans in place
4	High	Scenario planning for key strategic risks performed Low enterprise level/process level capabilities to address risks Responses partially implemented or not achieving control objectives Some contingency or crisis management plans in place
3	Medium	Stress testing and sensitivity analysis of scenarios performed Medium enterprise level/process level capabilities to address risks Responses implemented and achieving objectives most of the time Most contingency and crisis management plans in place, limited rehearsals
2	Low	Strategic options defined Medium to high enterprise level/process level capabilities to address risks Responses implemented and achieving objectives except under extreme conditions Contingency and crisis management plans in place, some rehearsals

1	Very Low	Real options deployed to maximize strategic flexibility High enterprise level/process level capabilities to address risks Redundant response mechanisms in place and regularly tested for critical risks Contingency and crisis management plans in place and rehearsed regularly[16]

Onset velocity is the time between a risk event occurring and the organization first recognizing its effects. Management measures onset velocity when planning and developing risk response programs.

An example of a risk onset velocity scale from COSO is shown below:

Rating	**Descriptor**	**Definition**
5	Very High	Very rapid onset, little or no warning, instantaneous
4	High	Onset occurs in a matter of days to a few weeks
3	Medium	Onset occurs in a matter of a few months
2	Low	Onset occurs in a matter of several months
1	Very Low	Very slow onset, occurs over a year or more[17]

When developing risk assessment criteria and assessing risks, management needs to differentiate between inherent risk and residual risk. COSO defines inherent risk as the organizational risk in the absence of any actions management might take to alter either the risk's likelihood or impact. Inherent risks are risks that controls are designed and implemented to mitigate. Residual risk is the risk remaining after management's risk response.

Applying this risk assessment differentiation is trickier than it might seem. Some entities interpret inherent risk to be the risk level assuming responses currently in place fail, and residual risk to be the level of risk assuming existing responses operate according to design. This approach focuses on control effectiveness in the current environment.

Other entities interpret inherent risk to be the current risk level assuming existing responses operate according to design and residual risk to be the estimated risk after responses under consideration are put into place. This approach focuses on evaluating risk response options. There is no one right answer and either approach may be useful depending upon the risk assessment purpose and the risk nature considered.

[16] https://www.researchgate.net/figure/5-Archisurance-risk-vulnerability-scale-based-on-Curtis-and-Carey-2012_tbl18_292994460

[17] https://www.researchgate.net/figure/6-Archisurance-risk-velocity-scale-based-on-Curtis-and-Carey-2012_tbl19_292994460

Assess Risks

Analyzing existing internal and external data can help individuals assess risk likelihood and impact. Sources of risk occurrence data include internal and external audit reports, public filings, insurance claims, and internal incurred loss event data including near misses, published reports by insurance companies, industry consortia, and research organizations. While relying on existing data provides objectivity, it's important to evaluate the relevance of the data under current and projected conditions. Adjustments may be warranted using expert judgment. In these cases, the rationale for adjustments must be clearly documented and communicated.

Using risk assessment criteria, management assesses risks by assigning values to each identified risk. This is often accomplished in two stages because not all risks are meaningfully quantifiable. First is a qualitative risk screening, followed by quantitative analysis of the most important risks. The qualitative assessment consists of assessing each risk according to descriptive scales described above. Quantitative analysis requires numerical values for both impact and likelihood using data from a variety of sources.

The analysis quality depends on the numerical value accuracy and completeness and the validity of the models used. Model assumptions and uncertainty should be clearly communicated and evaluated using techniques such as sensitivity analysis.

Both qualitative and quantitative techniques have advantages and disadvantages. Most enterprises begin with qualitative assessments and develop quantitative capabilities over time as their decision-making needs evolve.

A comparison of qualitative and quantitative risk measurement techniques from COSO is shown below:

Technique	**Advantages**	**Disadvantages**
Qualitative	Is relatively quick and easy Provides rich information beyond financial impact and likelihood such as vulnerability, speed of onset, and non-financial impacts such as health and safety and reputation Is easily understood by a large number of employees who may not be trained in sophisticated quantification techniques	Gives limited differentiation between levels of risk (i.e. very high, high, medium, and low) Is imprecise – risk events that plot within the same risk level can represent substantially different amounts of risk Cannot numerically aggregate or address risk interactions and correlations Provides limited ability to perform cost-benefit analysis
Quantitative	Allows numerical aggregation taking into account risk interactions when using an "at risk" measure such as Cash Flow at Risk Permits cost-benefit analysis of risk response options	Can be time-consuming and costly, especially at first during model development Must choose units of measure such as dollars and annual frequency which may result in qualitative impacts being overlooked

	Enables risk-based capital allocation to business activities with optimal risk-return Helps compute capital requirements to maintain solvency under extreme conditions	Use of numbers may imply greater precision than the uncertainty of inputs warrants Assumptions may not be apparent

For qualitative risk assessments, the most commonly used assessment techniques are:

- interviews
- cross-functional workshops
- surveys
- benchmarking
- scenario analysis

Risk assessment can be conducted through one-on-one interviews or facilitated meetings. Interviews are more appropriate for senior management, board members, and senior line managers due to their time constraints.

Cross-functional workshops are preferable to interviews or surveys because they enhance thinking about risk interactions and breaks down silo thinking. In addition, workshops improve risk understanding by bringing together diverse perspectives. For example, when considering a risk such as information security breach, workshop participants from information technology, legal and compliance, public relations, customer service, strategic planning, and operations management each bring different information regarding causes, consequences, likelihoods, and risk interactions. The downside to workshops is they do not work well in organization cultures that suppress free sharing of information or divergent opinions.

Surveys are useful for large, complex, and geographically-distributed enterprises or in organizations where the culture suppresses open communication. Survey results can be downloaded into analytical tools allowing risks and opportunities to be viewed by hierarchy level (board members, executives, managers), by business unit, by geography, or by risk category.

Survey drawbacks are response rates are often low. Response quality can be low if respondents give survey questions superficial attention in a rush to completion or if respondents misunderstand a question and don't have the opportunity to seek clarification. Also, anonymous surveys make it difficult to identify information gaps. The biggest drawback, however, is that survey respondents don't benefit from cross-functional discussions which enhance people's risk awareness and understanding, provide context and information to support the risk ratings, and consider risk interactions across silos. For these reasons, surveys should not be considered a substitute for workshops and other techniques for in-depth analysis of key risks.

Companies use **benchmarking** to assess risk likelihood and impact of potential events across an industry. It is a collaborative process among a group of entities that focuses on specific events or processes, compares measures and results using common metrics, and identifies improvement opportunities. Benchmarking produces data on events, processes, and measures for comparison with organization performance.

Sources of benchmarking data are research organizations, industry consortia, insurance companies and rating agencies, government agencies, and regulatory and supervisory bodies. For example, an oil field services company might benchmark its safety risk using measures such as lost time injuries using data for similar companies available from the Bureau of Labor Statistics, the Occupational Health and Safety Administration (OSHA), the American Petroleum Institute (API), or others.

Scenario analysis, traditionally recognized for its strategic planning usefulness, is also useful for assessing risks and linking risks back to strategic objectives. In scenario analysis, the analyst defines one or more risk scenarios, details key assumptions (conditions or drivers) that determine impact severity, and estimates the impact on a key objective. Scenarios can be developed jointly by risk owners and ERM personnel and built out and validated with specialists from various functions and management.

In the following COSO example, management conducted a scenario analysis to understand earnings risk and what events could negatively impact earnings. The example identified six scenarios impacting earnings, determined causal factors (such as price or volume changes or state of the economy), calibrated detailed assumptions, and estimated the earnings impact. Scenarios can be developed jointly by risk owners and ERM personnel and built out and validated with specialists from various functions and management.

Scenario Description	**Detailed Assumptions**	**EBIT Impact ($MM)**
Currency changes impact competitive landscape	15% volume decrease 20% price decrease Sustained for 9 months Recovery takes additional 9 months	- $500
Natural gas prices increase	$5/MM Btu increase Sustained for 12 months No ability to pass through increase	- $150
Crude oil prices increase	100% increase Sustained for 3 months Pass through 25% of cost increase	- $15
Technology shift	15% volume decrease/year 15% price decrease/year $2MM less in R&D expenditures	- $275
Competitive pressure	10% price decrease Sustained for 24 months	- $200

Supply chain disruption	10% volume decrease Sustained for 6 months	- $175

Source: Frederick Funston and Stephen Wagner, Surviving and Thriving in Uncertainty (Hoboken, NJ: John Wiley & Sons, Inc., 2010), 69.

Quantitative techniques include the above benchmarking and scenario analysis. It adds generating deterministic models showing forward-looking point estimates which are then used to generate probabilistic models of forward-looking distributions. Some of the most powerful enterprise-wide probabilistic models standpoint include causal at-risk models used to estimate gross profit margins, cash flows, or earnings over a given time horizon at given confidence levels.

Causal at-risk models include cash-flow-at-risk and earnings-at-risk metrics identifying specific risk factors driving future cash flow or earnings uncertainty. Causal at-risk models provide insight into how historical relationships might become uncoupled and deviate meaningfully from expectations.

Each risk factor can be modeled in detail and incorporated into the overall model. The model results in better risk measurement and management by showing how each risk factor could vary in the future and impact cash flow or earnings. Causal models produce added insight of the risk factors driving uncertainty which is an advancement from simply extrapolating past relationships in a pro-forma approach.

In reality, both pro-forma models built around historical ratios and causal at-risk models can be helpful and should be seen as complementary views of an uncertain future. Regardless of the model type used, the analyst needs to clearly disclose the confidence placed on risk level estimates and assumptions made in the model.

Model inputs may be derived from past records, relevant experience, published literature, market research, public consultation, experiments and prototypes, as well as economic, engineering or other models. In situations where historical data are not available, not relevant, or incomplete, the analyst may use a scientific consensus methodology called "expert elicitation". Expert elicitation is commonly used to estimate reasonable probabilities for low-likelihood, high-impact events. The downside to experts is that it is difficult to identify and address biases.

Assess Risk Interactions

Risks, themselves, and organization risks generally tend to be interrelated. Rarely do risks exist in isolation. Seemingly insignificant risks when isolated have the potential to interact with other risks, events, and conditions to become large enough to rise in the priority level because its impact size or occurrence likelihood builds. As a result, next management assesses risk interactions.

ERM enables an integrated and holistic view of risks which is important because the whole does not equal the sum of the parts. To understand portfolio risk, one must understand the individual element risks plus the interactions of individual elements due to the presence of natural hedges and mutually amplifying risks. Understanding risk interactions and then managing them requires breaking down silos.

A simple way to consider risk interactions is to group related risks into a broad risk area and then assign ownership and oversight for the risk area. An example would be grouping sourcing, distribution channel, and vendor concentration risks into a broader supply chain risk.

Three methods to identify risk interactions are:

- risk interaction map
- correlation matrices
- bow-tie diagrams

A risk interaction map is a simple matrix which has the same risks in the X and the Y axes. A symbol, such as “X”, is placed to indicate a risk interaction.

If historical data are available, risk interactions can be expressed quantitatively using a correlation matrix. This is an especially useful technique to apply within a risk category such as market risk. Difficulties in determining correlations for risks include the possibility that past causal relationships will not be indicative of future relationships, lack of historical data, differences in time frames (short-, medium-, and long-term), and the large numbers of risks required for an enterprise-wide assessment.

The following matrix from COSO shows a risk interaction map.

RISK	Supply Chain Disruption	Customer Preference Shift	Copper Price Increase > 25%	Work Stoppage > 1 Week	Economic Downturn	Supplier Consolidation	Local Competitor Enters Market	New Substitutes Available	Cost of Capital Increases > 5%	Tighter Emission Standards	FCPA Violation	Exchange Rate Fluctuations
Supply Chain Disruption			X	X	X	X	X					
Customer Preference Shift					X		X	X		X		X
Copper Price Increase > 25%	X				X	X						X
Work Stoppage > 1 Week	X				X	X					X	
Economic Downturn	X	X	X	X		X	X	X	X		X	X
Supplier Consolidation	X		X	X	X				X			
Local Competitor Enters Market	X	X			X							X
New Substitutes Available		X			X					X		
Cost of Capital Increases > 5%					X	X						X
Tighter Emission Standards		X						X				
FCPA Violation				X	X							
Exchange Rate Fluctuations		X	X		X		X		X			

[18]

Big-picture tools that can identify and assess risk responses, key risk indicators, and risk interactions are diagrams that break a complex risk occurrence into its component parts. Furthermore, these tools identify the chains of events that could lead to or result from the occurrence. The diagrams can be qualitative or serve as the basis for quantitative models.

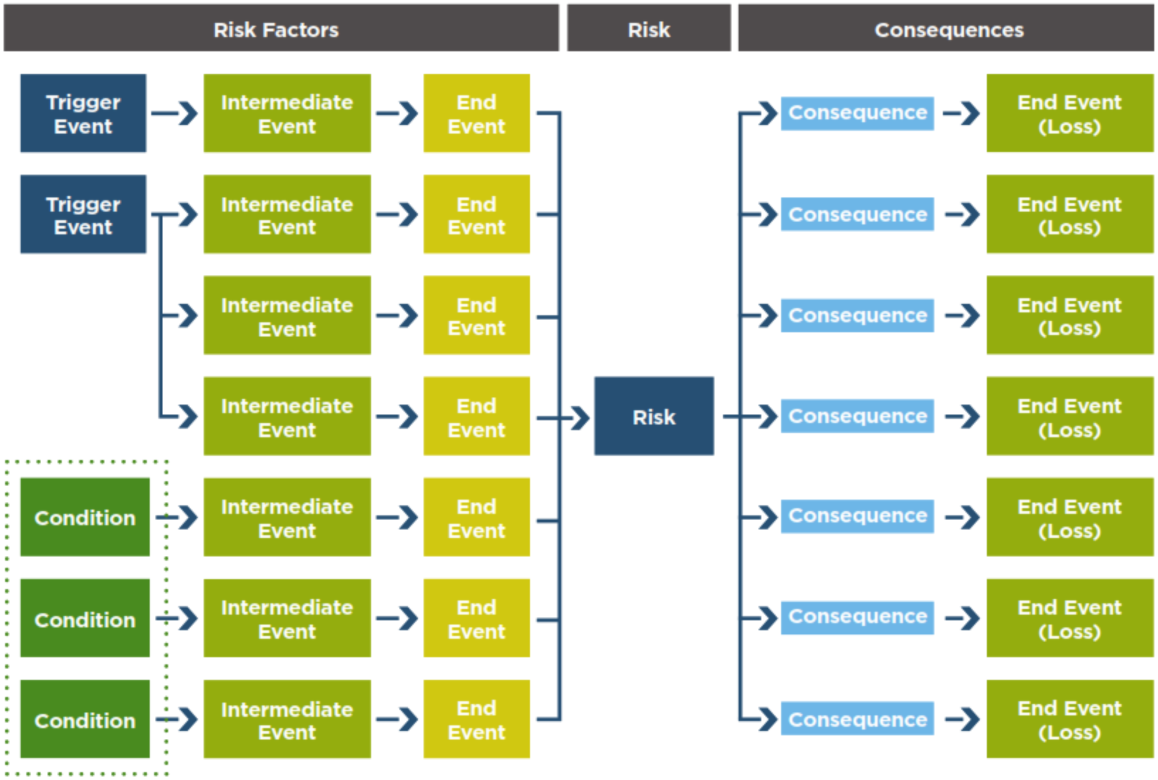
Three tools are:

- **Fault trees** – analyzes events or combinations of events that might lead to a hazard or an event
- **Event trees** – models sequences of events arising from a single risk occurrence
- **Bow-tie diagram** – combines a fault tree and an event tree and takes its name from its shape (in practice these three diagram names are often used interchangeably).

[18] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

Probabilistic models built on bow-tie diagrams are versatile for quantifying inherent and residual risk levels and performing what-if, scenario, and sensitivity analyses.

The following bow-tie diagram example is from COSO.



[19]

Prioritize Risks

Once management assesses the identified risks including documenting risk interactions, management next prioritizes the risks. The prioritized risk list becomes the basis for the final step of formulating risk responses and disclosing risks to different stakeholders.

Similar to assessing risks, management ranks and prioritizes the risk list using a two-step quantitative and qualitative process.

1. Quantitative. Rank risks according to single or multiple criteria, such as impact size multiplied by occurrence likelihood or impact size multiplied by vulnerability. A common approach is then comparing risk levels on the identified risk list with predetermined target risk levels and/or risk tolerance thresholds (the gap between current and desired risk level).

2. Qualitative. Review the ranked-risk order from #1 by considering more-subjective qualitative factors such as health, safety, reputation, vulnerability, or onset speed.

[19] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

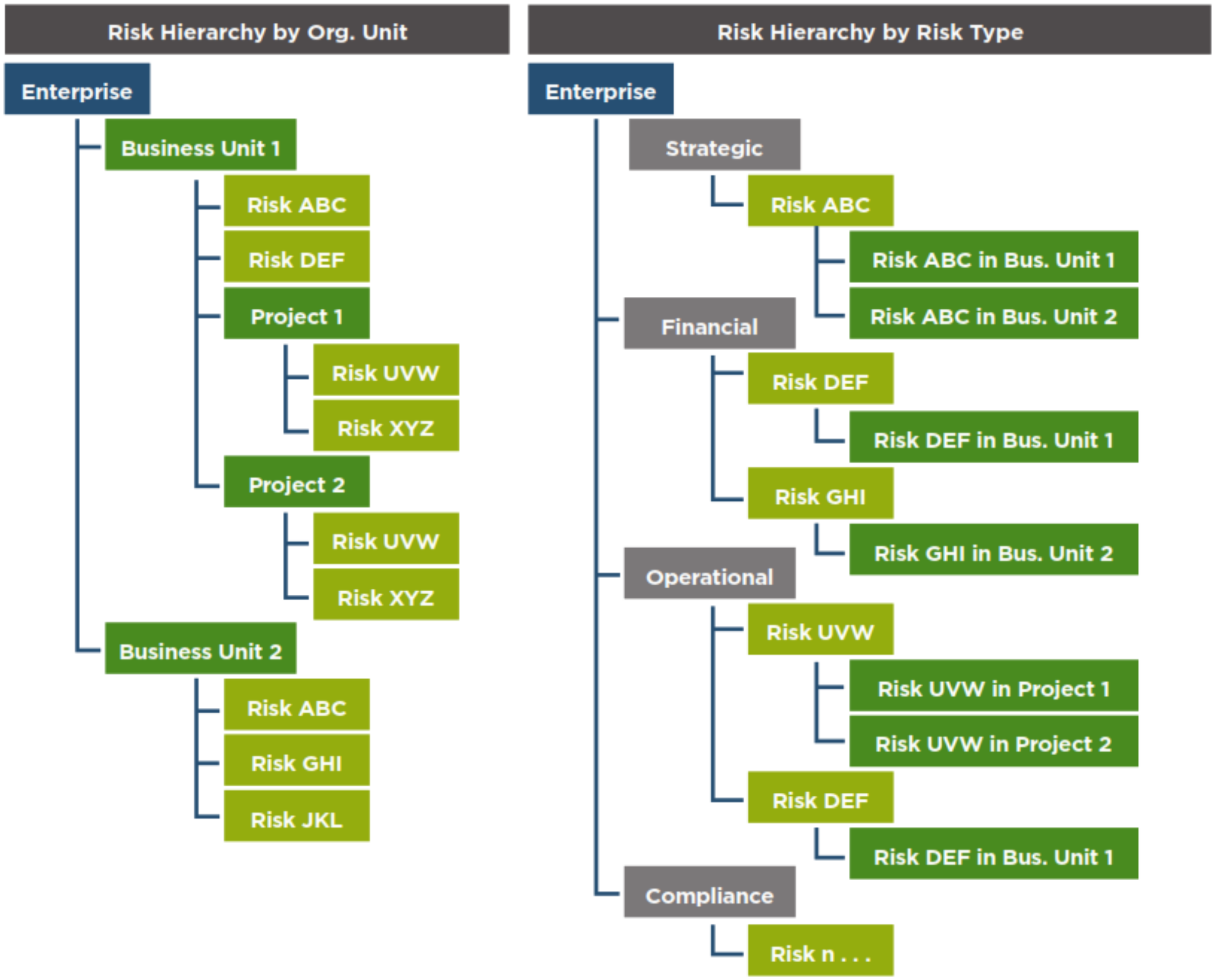
The term risk profile represents the entire portfolio of risks facing the enterprise. Some entities represent this portfolio as a hierarchy, some as a collection of risks plotted on a heat map. Entities with more mature ERM programs and quantitative capabilities may aggregate individual risk distributions into a cumulative loss probability distribution and refer to that as the risk profile.

There are two common methods of presenting aggregate organization risks (risk portfolio).

- Risk hierarchy
- Combined risk and opportunity map
- Heat map
- Mitigate, Assure, Redeploy, Cumulative Impact (MARCI) chart

One risk aggregation method is organizing risks according to a **hierarchy**. This is common in risk management systems where risks can be organized by organizational unit, risk type, geography, or strategic objective. The better risk management systems allow users to roll up and drill down for analysis and reporting. This provides a complete listing of the assessed risks but does not help with prioritizing.

The following risk hierarchy example is from COSO:



[20]

A second risk aggregation method is to view the risk portfolio as a **risk map**, also called a heat map. These are usually two-dimensional representations of risk **impact** size plotted against risk **occurrence likelihood**. Risk maps also can depict other relationships such as impact size versus vulnerability. As an enhancement, data point size can reflect a third variable such as onset speed or the estimate **degree of uncertainty**.

A very common risk prioritization method is designating a risk level for each area of the graph such as very high, high, medium, or low. The higher the combined size impact and occurrence likelihood ratings, the higher the overall risk level. The acceptable boundaries between these levels vary from entity to entity depending on risk appetite. For example, an entity with a greater risk appetite will have boundaries between risk levels shifted toward the upper right, and an entity with greater risk aversion will have boundaries between risk levels shifted toward the bottom left.

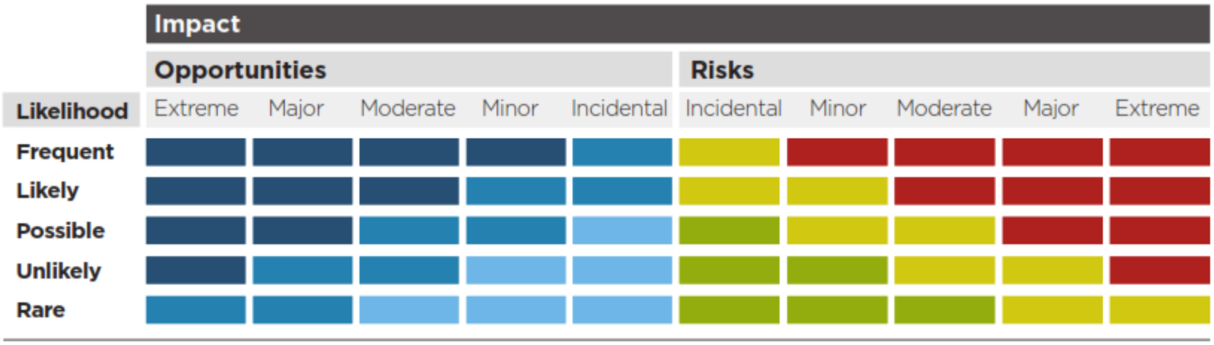
[20] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

Also, some entities adopt asymmetric boundaries placing a somewhat greater emphasis on impact than on likelihood. For example, a risk having an impact rating of moderate and likelihood rating of frequent has an assigned risk level of high, whereas a risk having an impact rating of extreme and a likelihood rating of possible has an assigned risk level of very high.

After plotting risks on the heat map, rank the risks from highest to lowest by level. These rankings may then be adjusted based on other considerations such as vulnerability, onset speed, or detailed knowledge of the nature of the impact. For example, within a group of risks having a designation of very high, those risks having extreme health and safety or reputational impacts may be prioritized over risks having extreme financial impacts but lesser health and safety or reputational impacts.

When using numerical ratings in a qualitative environment, it’s important to remember that the numbers are labels and not suitable for mathematical manipulation although some entities do multiply the ratings, such as for impact and likelihood, to develop a preliminary ranking.

Where entities have defined impact scales for both opportunities and risks, they may plot risks on a map such as that illustrated below. This allows a direct comparison of the highest rated opportunities and risks for consideration and prioritization.



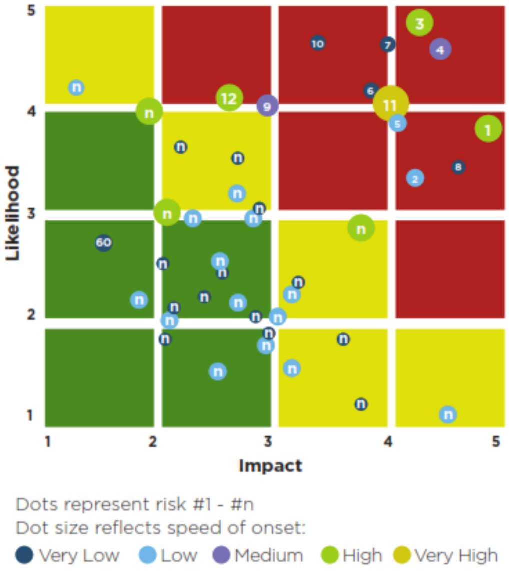
[21]

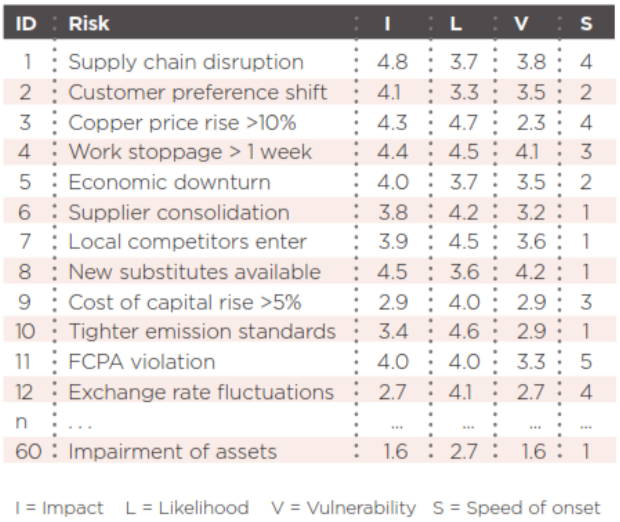
[21] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

COMPREHENSIVE EXAMPLE

Consider the following COSO example: A company identified 60 risks in its risk universe. It then determined appropriate assessors. It used a combination of interviews, workshops, and a survey to perform an initial qualitative assessment of impact, likelihood, vulnerability, and onset speed criteria.

The company evaluated risk interactions which refined the highest risks and assessments. Next, the company plotted risks on a heat map to perform an initial prioritization. Twelve risks plotted in the 'Very High' risk level designated as red in the heat map. These risks were designated 'key' risks meaning that they will be reported to and monitored by executive leadership and the board of directors.





ID	Risk	I	L	V	S
1	Supply chain disruption	4.8	3.7	3.8	4
2	Customer preference shift	4.1	3.3	3.5	2
3	Copper price rise >10%	4.3	4.7	2.3	4
4	Work stoppage > 1 week	4.4	4.5	4.1	3
5	Economic downturn	4.0	3.7	3.5	2
6	Supplier consolidation	3.8	4.2	3.2	1
7	Local competitors enter	3.9	4.5	3.6	1
8	New substitutes available	4.5	3.6	4.2	1
9	Cost of capital rise >5%	2.9	4.0	2.9	3
10	Tighter emission standards	3.4	4.6	2.9	1
11	FCPA violation	4.0	4.0	3.3	5
12	Exchange rate fluctuations	2.7	4.1	2.7	4
n	. . .	...	...	...	...
60	Impairment of assets	1.6	2.7	1.6	1

I = Impact L = Likelihood V = Vulnerability S = Speed of onset

[22]

The **MARCI** (for Mitigate, Assure, Redeploy, and Cumulative Impact) **chart** is another useful risk prioritization tool, especially when the primary purpose of the prioritization exercise is for risk response. Risks plotting the farthest in the upper right quadrant represent the highest impact and vulnerability and would benefit the most from additional management effectiveness in managing the risks.

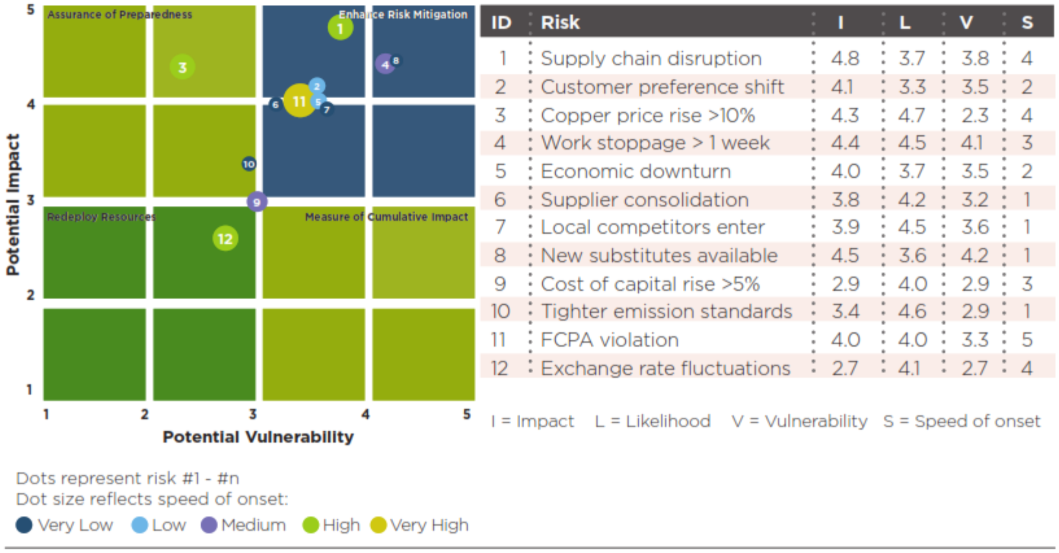
The MARCI chart plots risks along the two axes of impact size and vulnerability, and indicates each risk's onset speed by the data point size.

COMPREHENSIVE EXAMPLE (CONTINUED)

Continuing our previous example from COSO, the 12 risks rated 'Very High' were plotted on a MARCI chart to further refine the prioritization and to perform a preliminary evaluation of the type of appropriate risk response. This shows how the company's hedging program reduces its vulnerability to copper price increases (risk 3) and evaluate its previous decision to not hedge against currency fluctuations (risk 12).

[22] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

Leadership can also see that supply chain disruption (risk 1) can occur with little warning and severe impact. This and the other risks in its quadrant require action to reduce vulnerability. The executive leadership team and board members will pay particular attention to management's actions to respond to these risks. The top 12 risks were tagged for further quantification and probabilistic modeling.



ID	Risk	I	L	V	S
1	Supply chain disruption	4.8	3.7	3.8	4
2	Customer preference shift	4.1	3.3	3.5	2
3	Copper price rise >10%	4.3	4.7	2.3	4
4	Work stoppage > 1 week	4.4	4.5	4.1	3
5	Economic downturn	4.0	3.7	3.5	2
6	Supplier consolidation	3.8	4.2	3.2	1
7	Local competitors enter	3.9	4.5	3.6	1
8	New substitutes available	4.5	3.6	4.2	1
9	Cost of capital rise >5%	2.9	4.0	2.9	3
10	Tighter emission standards	3.4	4.6	2.9	1
11	FCPA violation	4.0	4.0	3.3	5
12	Exchange rate fluctuations	2.7	4.1	2.7	4

I = Impact L = Likelihood V = Vulnerability S = Speed of onset

[23]

Aggregating in a quantitative environment is for situations where key risks have been quantified using a common measure such as financial loss or an at-risk measure. It is possible to aggregate these individual probability distributions into a single distribution reflecting correlations and portfolio effects. Measures that are gaining traction for this purpose are gross margin at risk, cash-flow-at-risk, and earnings-at-risk.

The primary applications for a single at-risk measure presenting an aggregate view of risk (over a given time horizon at a specified confidence level) are capital allocation, solvency assessments, risk utilization measures, and capacity-relative-to-risk-appetite. Risk aggregation models are extremely variable from one enterprise to another, even within a single industry such as the financial services industry.

Risk Response

Last in the risk assessment process is management developing risk responses. This step includes determining whether to accept, reduce, share, or avoid the risk; performing a cost-benefit analysis, formulating a response strategy, and developing response plans for each risk.

[23] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

Summary – Practical Tips

Risk management success depends upon executive commitment, process understandability, internal communication clarity, and organization resources. Risk assessment processes must be performed by management and employees possessing the right skills and be supported by information technology.

Best practices for ERM is a hybrid top-down and bottom-up approach. From the top-down, a central corporate ERM function (or part of a senior manager's responsibility in a small organization) defines common standards, oversees risk assessments across business units, and coordinates risk interaction analysis. The central ERM function senior manager (or department in larger organizations) needs skills in facilitation, project management, analysis, and risk management practices.

From the bottom-up, ERM includes operating management and employees in positions closest to the risks. These individuals are process owners, and, accordingly, risk owners. Risk owners ultimately bear responsibility for assessing risk levels and developing and implementing risk response plans to manage risks within tolerable levels.

This hybrid top-down and bottom-up approach brings the best of both worlds achieving consistent and comprehensive risk management coverage while embedding accountability and leveraging expertise of the individuals nearest to the risks.

For risk management efficiency, management and employees must be supported by the right technology. Spreadsheets can be practical in the early phases of risk management; however, automated system controls improve control implementation, increase control effectiveness, enables more thorough monitoring, and make the risk management process more efficient.

COSO's Enterprise Risk Management – Integrated Framework emphasizes the need to assess and oversee risks from a holistic organization perspective. The risk management process exists within a larger framework that uses the information gleaned to make decisions about risk responses and monitoring, and feeds information back into the strategic planning process.

The ERM function must be empowered to monitor and oversee implementation of risk responses. If participants don't see that their contributions and hard work during risk assessment lead to concrete actions that make a real difference, all employees may become cynical and less engaged.

You'll know you're doing risk assessment right when leaders at every level use risk management to make decisions regarding value.

COSO FRAMEWORK PRINCIPLES – RISK ASSESSMENT

This section addresses the COSO framework's four principles related to the risk assessment process:

Principle 6 – Specify suitable financial reporting objectives

Principle 7 – Identify and analyze risks of achieving these financial reporting objectives

Principle 8 – Assess fraud risk

Principle 9 – Identify and assess significant changes

Principle 6. The Organization Specifies Objectives with Sufficient Clarity to Enable the Identification and Assessment of Risks Relating to Objectives

Objectives can be expressed clearly and distinctly. The challenge is identifying risks of not achieving objectives. Starting with objectives it becomes more certain to determine that relevant risks have been identified.

In addition to financial statement objectives, we have discussed previously that operating objectives also impact financial statements. For example, the board's risk appetite impacts product warranty reserves, the allowance for doubtful accounts, the allowance for aggressive tax positions, etc.

Compliance objectives also impact financial statements in fines and penalties as well in disclosures.

EXAMPLE

On May 25, 2018, a sweeping new European Union (EU) directive went into effect called the General Data Protection Regulation (GDPR).

GDPR is a significant regulatory change to data privacy laws and have implications for U.S. companies because all organizations that have an Internet presence and conduct business within the EU must comply with the regulation. It protects EU residents and citizens (this includes Americans living there; however, if you're a European living in the U.S., you're not protected).

GDPR expands what counts as personal data and your rights over that data. Your data includes what you post on social media, your electronic medical records, and your mailing address, your IP address, and GPS location.

This law generally requires consent before processing of personal data. A company can't just sign you up without explicitly asking. Biometrics which is considered special category data under the law, requires a more rigorous form.

Failure to comply with GDPR could have serious negative consequences to an organization's bottom line, customer and supplier relationships, brand image, and reputation.

GDPR has substantial fines and penalties for non-compliance. There are two tiers of fines: Up to GBP10 million or 2% of annual global revenue of the previous year, whichever is higher and up to GBP 20 million pounds or 4% of annual global turnover, whichever is greater.

It is expected that breaches of data subjects' rights will result in the higher level fine, although many factors will help determine the actual fine including the duration and gravity of the infringement and the types of personal data affected. The level of cooperation and behavior of the organization will also play a role in influencing the final fines.

Equifax incurred one of the largest data breaches in 2017. Equifax' data breach included the personal information of 143 million and Equifax failed to meet the GDPR 72-hour breach notification requirement when the breach became public in September 2017.

If GDPR had been in force at that time, the higher-level fine would have been $124 million based on 4% of Equifax' 2016 reported revenue of $3.1 billion.

COSO Principle 6 has 15 focus points covering financial reporting, compliance, and operational areas. Each of these points does not require separate controls because many are interrelated; some controls may mitigate more than one point.

Operations Objectives

1. Reflects management's choices – operations objectives reflect management's choices about entity structure, industry, and operating performance.

2. Considers risk tolerances – management considers the acceptable levels of risk relative to achieving operational goals and objectives.

3. Includes operations and financial performance goals – the organization reflects the desired level of operations and financial performance for the entity within operations objectives.

4. Forms a basis for committing of resources – management uses operations objectives as a basis for budgeting and prioritization needed to attain desired operations and financial performance.

External Financial Reporting Objectives

1. Complies with applicable accounting standards – financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate for the circumstances.

2. Considers materiality – management considers materiality in financial statement presentation. The materiality concept is rooted in user needs.

3. Reflects entity activities accurately and clearly – external reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.

External Non-Financial Reporting Objectives

1. Complies with externally-established standards and frameworks – management establishes objectives consistent with laws and regulations, or standards and frameworks of recognized external organizations.

2. Considers the required level of precision – management reflects the required level of precision and accuracy suitable for user needs and as based on criteria established by third parties in nonfinancial reporting.

3. Reflects entity activities accurately and clearly – external reporting reflects the underlying transactions and events within a range of acceptable limits.

Internal Reporting Objectives

1. Reflects management and the board's choices – internal reporting provides management with accurate and complete information regarding and consistent with management's choices and information needed in managing the entity.

2. Considers the required level of precision – management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.

3. Reflects entity activities – internal reporting reflects the underlying transactions and events within a range of acceptable limits.

Compliance Objectives

1. Reflects external laws and regulations (or contracts and grants provisions, if applicable) – laws and regulations establish minimum standards of conduct that the entity integrates into compliance objectives.

2. Considers risk tolerances – management considers the acceptable levels of risk relative to achieving various compliance objectives.

EXAMPLE

Specifying Objectives

The board of directors and management of Seaboard Yacht Charter LLC set an overall financial reporting objective of preparing reliable financial statements in conformity with U.S. GAAP. Then management set more detailed financial reporting objectives and sub-objectives for major accounts and activities of Seaboard's multinational operations, including financial statement assertions, accounting policies and qualitative characteristics of accounts and activities.

For example, management has created objectives related to the existence and completeness of financial statement assertions of related transactions in the areas of sales, purchasing, and payroll.

These objectives and sub-objectives are reviewed annually by financial management, taking into account their continued relevance and suitability to the company's accounts and activities, as well as environmental changes such as issuance of new or revised accounting standards or changing commercial trends.

Principle 7. The Organization Identifies Risks to the Achievement of Its Objectives across the Entity and Analyzes Risks as a Basis for Determining How the Risks Should Be Managed

This COSO principle covers identifying risks of not achieving the objectives specified in principle 6. These identified risks will become the basis for assessing how well the actual control activities mitigate risks (COSO principle 10). Management needs to identify specific potential risks to not achieving objectives.

COSO principle 7 has five focus points.

1. Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels – the organization identifies and assesses risks at all the levels relevant to achieving objectives

   Entity-level risk identification is at a high level and does not include assessing transaction-level risks. Process-level risk identification is more detailed and includes transaction-level risks. Management also assesses risks from outsourced service providers, key suppliers, and channel partners.

2. Analyzes Internal and External Factors – risk identification considers both internal and external factors and their impact on achieving objectives

   - Management realizes that risk is dynamic and considers the rate of change in risks. If a rate of change increases, management will accelerate its risk assessment frequency.

   - Management evaluates the external factors affecting entity-level risk including:

     - Economic
     - Natural environment
     - Regulatory
     - Foreign operations
     - Social
     - Technological

   - Management evaluates the internal factors affecting entity-level risk including:

     - Infrastructure and use of capital resources
     - Management structure
     - Personnel, including quality, training and motivation
     - Access to assets, including possibilities for misappropriation
     - Technology, including possibility of IT disruption

   - Management solicits input from employees as to transaction-level risks (also see control activities).

EXAMPLE

A health care company identified risks related to patient safety, compliance with Medicare regulations and existence of patient service revenue. The auditor is concerned with risks related to the existence of patient service revenue but is only concerned with compliance with Medicare regulations or patient safety as it relates to a risk of material misstatement of the financial statements.

External Risks	**Internal Risks**
Change in the way health care entities deliver service (i.e., outpatient procedures taking the place of inpatient procedures), less invasive techniques being used. Other competitive pressures such as ambulatory surgi-centers taking volume away from hospitals.	Failures due to technology such as entity growth without sufficient investment in IT to keep up with volume or new IT system such as substantial growth in a health plan hinders its ability to process claims and forecast the amounts incurred but not reported.
Changes in the regulatory environment that are unfavorable to the entity such as change in safety standards that render equipment obsolete or changes in certificate of need laws that make expansion impossible.	Changes in personnel practices such as shortage of certain employee types such as nurses, termination of training programs due to cost or morale issues.
Natural disasters, for example, lack of a disaster recovery program.	Nature of organization's control activities such as change from manual to programmed controls.
Changes in accounting pronouncements such as those related to investments.	New personnel Restructurings or acquisition of additional facilities.

3. Involves Appropriate Levels of Management – the organization puts into place effective risk assessment mechanisms that involve appropriate management levels

   – Effective risk assessment mechanisms match an appropriate level of management expertise to each risk.

4. Estimates Significance of Risks Identified – analyze identified risks to estimate the risk potential significance. Management assesses potential risk severity using concepts of occurrence likelihood, impact magnitude, vulnerability, and onset velocity.

   – Management assesses the significance of risks using criteria such as:

     - Likelihood of risk occurring and impact

     - Velocity or speed to impact upon occurrence of the risk

     - Persistence or duration of time of impact after occurrence of risk

5. Management Determines How to Respond to Risks – risk assessment includes considering how to manage the risk and whether to accept, avoid, reduce, or share the risk.

   – Risk responses fall within the following categories:

    - Acceptance – no action taken
    - Avoidance – exiting the risky activities
    - Reduction – action taken to reduce likelihood, impact, or both

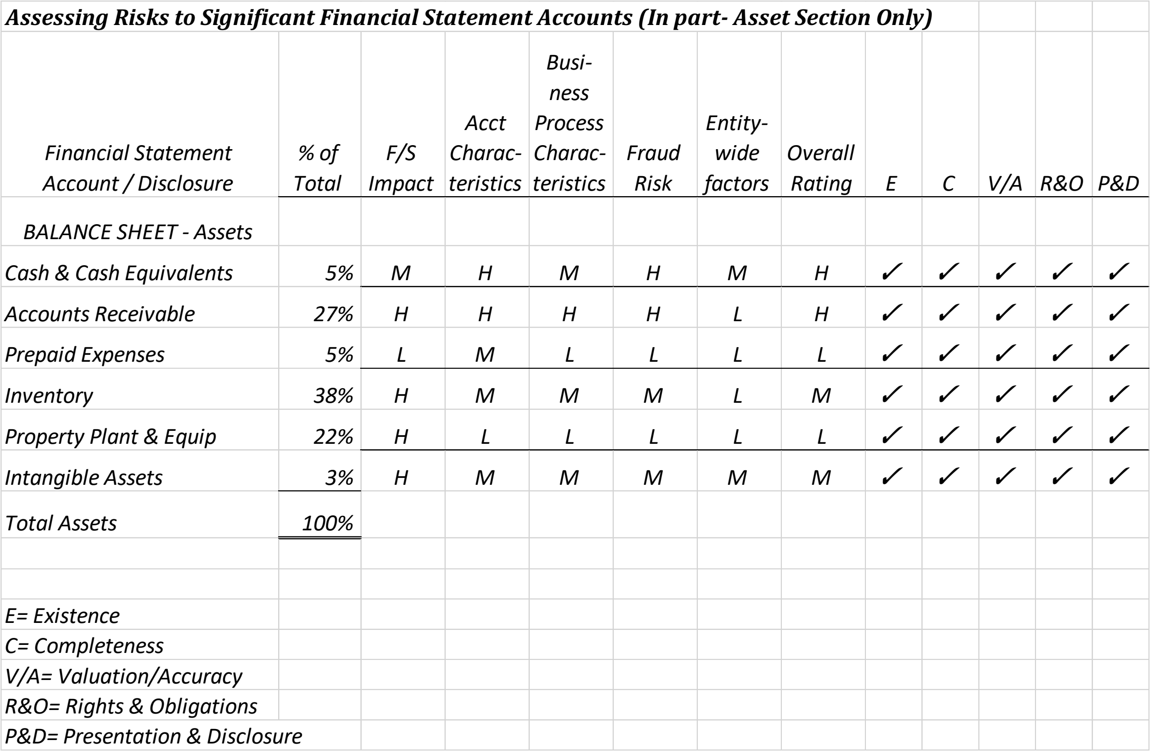
- Sharing – transferring part of the risk, for example, insurance, joint venture, hedging, or outsourcing
- In relation to risk responses, management should consider:
    - Which response aligns with entity's risk tolerance
    - Segregation of duties needed to get intended significance reduction
    - Cost/benefit of response options

EXAMPLE

Assessing Risks to Significant Financial Statement Accounts

Management at Tall Peaks Outfitters considers risks to achieving their financial reporting objectives. They review each significant financial statement account and disclosure, and link each account balance to the relevant financial statement assertion.

The resulting risk assessment spreadsheet is illustrated, in part:



Assessing Risks to Significant Financial Statement Accounts (In part- Asset Section Only)

Financial Statement Account / Disclosure	*% of Total*	*F/S Impact*	*Acct Charac-teristics*	*Business Process Charac-teristics*	*Fraud Risk*	*Entity-wide factors*	*Overall Rating*	*E*	*C*	*V/A*	*R&O*	*P&D*
BALANCE SHEET - Assets												
Cash & Cash Equivalents	*5%*	*M*	*H*	*M*	*H*	*M*	*H*	✓	✓	✓	✓	✓
Accounts Receivable	*27%*	*H*	*H*	*H*	*H*	*L*	*H*	✓	✓	✓	✓	✓
Prepaid Expenses	*5%*	*L*	*M*	*L*	*L*	*L*	*L*	✓	✓	✓	✓	✓
Inventory	*38%*	*H*	*M*	*M*	*M*	*L*	*M*	✓	✓	✓	✓	✓
Property Plant & Equip	*22%*	*H*	*L*	*L*	*L*	*L*	*L*	✓	✓	✓	✓	✓
Intangible Assets	*3%*	*H*	*M*	*M*	*M*	*M*	*M*	✓	✓	✓	✓	✓
Total Assets	*100%*											
E= Existence												
C= Completeness												
V/A= Valuation/Accuracy												
R&O= Rights & Obligations												
P&D= Presentation & Disclosure												

EXAMPLE

Considering Changes in Information Systems

Das Gupta Engineering Ltd. manufactures marine parts, components and sub-systems, with operations in eleven states. Ram Gupta, the CEO, conducts monthly meetings with senior managers to solicit their insights, and present his, on any newly-identified risks. This includes risks related to changes in activities, systems, or personnel processes, as well as any others that may impact financial reporting. The group then develops response strategies to address these new risks.

Principle 8. The Organization Considers the Potential for Fraud in Assessing Risks to the Achievement of Objectives

What Is Fraud?

Most people involved in the fraud-fighting business have their own concept of what fraud is – and what it isn't. As a result, we have a grab bag of definitions to choose from in guiding our day-to-day work. Some are legal definitions, others are academic, while still others are based on personal experience. Out of the lot, the most useful definitions boil down to two.

According to the Association of Certified Fraud Examiners (ACFE), fraud is:

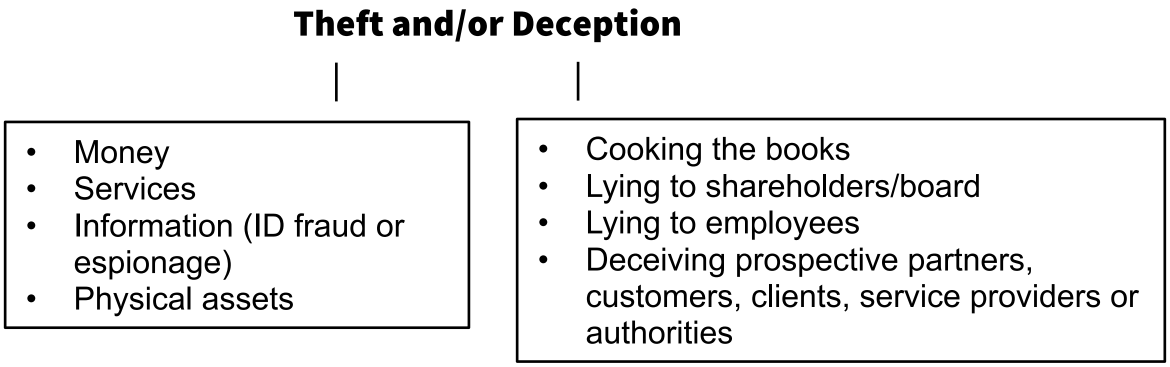
> "Any illegal acts characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the application of threat of violence or of physical force. Frauds are perpetrated by individuals and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."[24]

According to the American Institute of Certified Public Accountants (AICPA), fraud is:

> "A broad legal concept that is distinguished from error depending on whether the action is intentional or unintentional."

Regardless of whose definition of fraud you accept, you will find that nearly all incidents of fraudulent activity – also called white-collar crime – fall into one or both of two categories: Theft and Deception. The following is a graphic illustration of this dual-category definition of fraud.

[24] Association of Certified Fraud Examiners 2014 Report to the Nations on Occupational Fraud and Abuse.



Theft and/or Deception

- Money
- Services
- Information (ID fraud or espionage)
- Physical assets

- Cooking the books
- Lying to shareholders/board
- Lying to employees
- Deceiving prospective partners, customers, clients, service providers or authorities

Myths and Realities about Fraud

A key reason for the seriousness of the fraud problem is that management often falsely believes the organization is adequately protected against fraud.

More precisely, many top executives like to think that because they have complied with laws and regulations requiring them to put internal controls in place, they are adequately protected against attacks by fraudsters.

In reality, *no* organization – no matter how well-designed its internal controls against fraud are – can ever be fully protected against determined fraudsters – either from outside or inside. The bad guys always find weaknesses in business processes and procedures that they can exploit to steal cash, forge checks, collude with vendors, falsify financial reports, steal confidential data, or commit any of a million other crimes that cause either financial or reputational damage – or both.

Additional management myths about fraud:

Myth #1: Ethics and Compliance Training "Has Us Covered." This myth assumes that such training addresses key issues about fraud and instructs employees how to detect the red flags of fraud and how to report it.

In fact, compliance and ethics typically have little to do with fraud. Nearly all organizations have a code of ethics on which employee training is based. However, most such codes don't even contain the word "fraud."

The typical code of ethics informs employees about issues such as sexual harassment, antitrust issues, accepting gifts from vendors, and other ethical issues that are important – *but are not related to fraud.*

While all fraud is unethical, not all unethical conduct is fraudulent.

EXAMPLE

Accepting a gift from a vendor – such as a paid vacation, tickets to professional sporting events, or similar items – is unethical and most likely in direct violation of an organization's ethics policy. However, such gifts are not necessarily illegal, and hence giving or receiving them often does not represent fraud.

Myth #2: Our Finance and Accounting Staff Are Qualified to Protect Us Against Fraud. Internal auditors, financial managers, accountants, treasurers, and other professionals in most organizations are usually *untrained* in fraud detection and prevention, and they are not trained – let alone expected to be – fraud investigators. However, in many organizations, there is growing pressure for internal auditors and other financial professionals to focus more on fraud detection.

Myth #3: We Have Very Little Fraud Here. This assumption is often made without quantitative proof. In too many organizations, senior management believes there is little fraud because it wants to believe that. In the meantime, employees, vendors, or customers could be stealing huge amounts of money.

CASE STUDY

Big-Dollar Check Fraud Scheme Challenges Jurors

Troy Moody of Hartford, CT, was sentenced by United States District Judge Janet Bond Arterton to 60 months in prison, followed by three years of supervised release, for his participation in a conspiracy to defraud Bank of America (BofA).

According to court documents and statements made in court, for nine months, Moody conspired with two BofA employees to steal business checks from the BofA lockbox processing center in East Hartford, CT.

The employees gave Moody at least three checks totaling approximately $390,000 that were stolen from the lockbox. Moody and his co-conspirators then induced other individuals to register businesses in the names of the payees on the stolen business checks…open bank accounts in the names of those payees…deposit the stolen checks into the fraudulent accounts, and then to withdraw the proceeds of the stolen checks before the banks or legitimate payees realized the checks had been stolen.

Moody pleaded guilty to one count of conspiracy to commit bank fraud.

Moody was previously involved in another bank fraud conspiracy. In 2001, he was sentenced to 68 months of imprisonment, followed by five years of supervised release.

Myth #4: Fraud Is a Necessary Cost of Doing Business. You may say, "Most organizations can afford a small amount of fraud because they are financially sound, and it may cost more to catch the fraudsters than to write off the losses." In other words, *fraud is part of the cost of doing business.*

When the fraudsters know that you do not take action against "small amounts of fraud," or raise awareness among employees about fraud, they are encouraged to attempt larger amounts.

If the organization has no policy for investigating and punishing fraudsters, it is effectively *inviting* dishonest people to steal.

So-called small frauds eventually accumulate into major losses. And when that occurs and the news media finds out about it, the reputational damage to the organization can be serious enough to drive away customers and attract attention from regulatory agencies that could seriously endanger the organization's financial health.

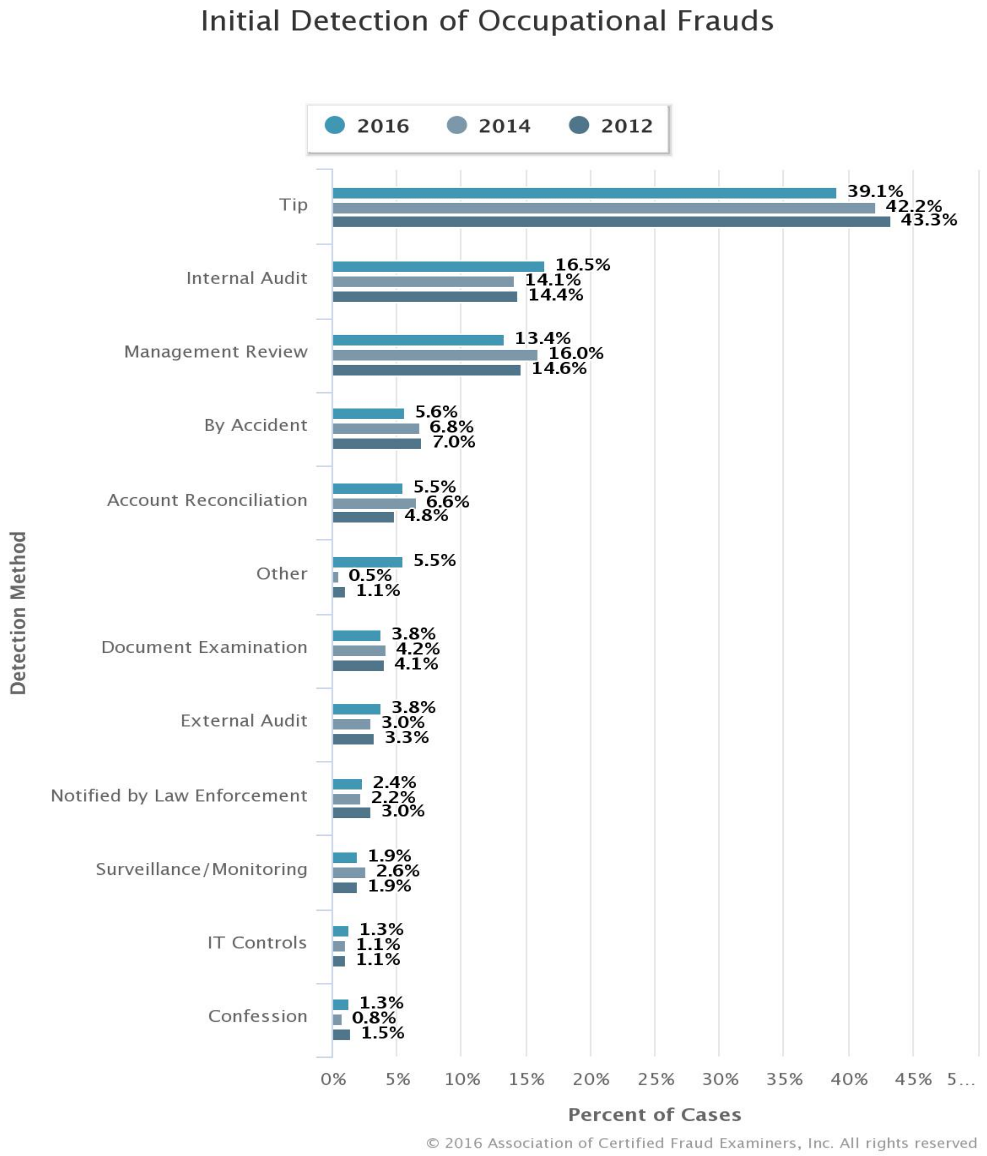
Myth #5: Implementing Controls and Anti-Fraud Training Is Costly. The reality is fraud losses are much costlier. If, as the ACFE has determined, your organization loses up to 5 percent of its gross revenue to fraud every year, you can quickly calculate how many actual dollars are lost to fraud each year.

The price of implementing the most effective anti-fraud controls – including financial controls, operational controls, physical security of inventory, employee training, tip hotlines, fraud risk assessments, audits, etc. – would never amount to more than a fraction of the money lost to fraud in any given year.

It is risky to assume that any organization is adequately protected against fraud. Even with the best controls in place, determined criminals will always find ways around them.

THE URGENCY OF DETECTING AND PREVENTING FRAUD

As you will see from the following example, internal audits and controls play a key role in the fraud detection. Unfortunately, because of their general lack of training in fraud detection, the role of internal auditors and other financial professionals in fraud detection is *not* as significant as it should be: detection by accident and by employee or outsider tip rank higher.



The sum of percentages exceeds 100 percent because in some cases respondents identified more than one detection method.
Source: *ACFE Report to the Nation on Occupational Fraud*, 2016.

Many frauds *can* be prevented. There are many ways to detect and report fraud before it does serious damage to the organization’s reputation and financial health.

To reduce the risk of being victimized by fraud, internal financial staff must play a decisive role in fraud detection. Today’s training will provide solid guidance on how to use audit and other detection methods to discover fraudulent activity in an organization and when and how to report it so that senior management can determine whether to launch investigations of incidents of fraud or take other measures to rid the organization of fraud.

THE HUMAN ELEMENT OF FRAUD

Who Commits Fraud?

Earlier, you were provided with an array of statistics illustrating the nature and magnitude of the fraud problem. One critical set of data *not* included is that defining *who* commits fraud. There is, for example, some disparity in the findings of recent research studies on how much of total fraud is committed by insiders compared with external perpetrators.

Some data put the ratio at 60–40; others come in closer at 80–20. In any case, while most research shows that on average, a majority of fraud committed against *all* U.S. organizations is internal, the actual ratio varies from one industry to the next … and from organization to organization.

One of the most recent studies – conducted by the prominent international fraud investigation firm, Kroll – concludes that regardless of industry, the average proportion of fraud committed by insiders is *67 percent*.

Who are the Bad Guys?

With external fraudsters, organizations have a dizzying variety of perpetrators to worry about. Their illegal exploits and how to detect and prevent them are discussed in coming sections. *The list of dishonest outsiders includes:*

- Dishonest customers (retail and commercial)
- Identity thieves/fraudsters
- Check forgers and counterfeiters
- Dishonest vendors
- Ex-employees
- Internet fraudsters (including phishing attackers, hackers, malicious code programmers and similar "cyber-criminals")
- Credit card fraudsters
- Crooked mortgage brokers, appraisers, and attorneys

Because external fraudsters are so varied in terms of both the business and social environments in which they operate, as well as their geographical location, it is difficult to identify common personal, behavioral, or demographic characteristics. Some are hardened career criminals; others are occasional opportunists; others target organizations for the "thrill of it"; still others do what they do out of desperation (which is increasingly the case during economic downturns, when, for example, banks regularly experience spikes in credit card fraud, identity-related frauds, and internet crime).

There are few if any behavioral or demographic characteristics common to external fraudsters. For that reason, this training will focus on the varieties of crimes they perpetrate and explain how to spot the red flags, *regardless* of who the perpetrators are.

The Insider Threat

Fortunately for fraud fighters, the same is not true with regard to internal fraudsters.

Employees who commit fraud *do* have common personality and behavioral traits. They are also prone to proven psychological influences that make them relatively easy to spot.

In general, research on internal fraud shows that about 80 percent of employees in any organization are fundamentally honest.

If that is the case, you may wonder, how can internal fraud be such a costly threat?

Many fraud prevention experts use the so-called **20–60–20 rule** to illustrate the human component of fraud:

- Twenty percent of the people in any organization will never steal – no matter what. They are individuals whose character and integrity are so incorruptible that nothing could pressure or tempt them to do anything dishonest.
- Sixty percent of the people in the organization are "fence sitters." They are basically honest people. But if given the *opportunity* to commit fraud and they perceive the risk to be minimal, they might cross the line.
- The remaining 20 percent are inherently dishonest. They will commit fraud whenever the opportunity arises. In fact, they often will look for or even *create* opportunities to steal or deceive if they think it will result in personal financial gain.

To understand the insider fraud threat, it is helpful to divide it into two key categories:

1. **Employee-level fraud.** This type of fraud is committed by people who are neither supervisors nor managers or executives. They may be salaried professionals or hourly employees.
2. **Management-level fraud.** These crimes are committed by managers at all levels, including the most senior echelons. Many of the frauds committed by these individuals are the same as those committed by employees lower down the organization chart.

Though committed with less frequency than employee-level fraud, virtually all management-level frauds result in much greater losses than those perpetrated at lower levels.

Managers have more authority and therefore more opportunity to cheat than those who work under them.

These statistics do not include fraud by business owners and top executives. While such frauds are committed with less frequency than those committed by managers and employees, frauds by the “top dogs” result in losses five times greater than those committed by managers and 11 times greater than those by employees.

The Fraud “Triangle”

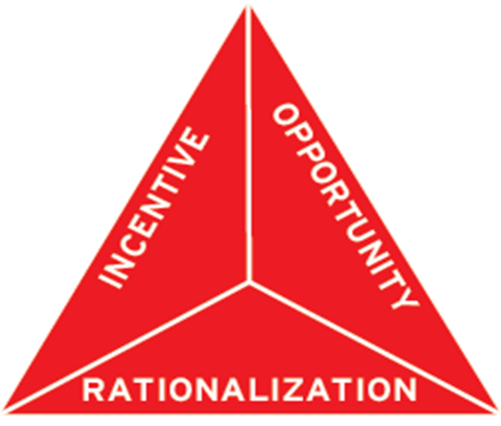
One set of factors common to internal fraudsters *at all levels in any organization* is the Fraud “Triangle”. The theory behind the Fraud “Triangle” was developed in the 1940s by a leading criminologist, Donald Cressey, who conducted extensive research with convicted embezzlers to determine what motivated seemingly honest people to commit fraud.

Cressey’s research led him to coin the term “trust violators” to describe people who embezzle. According to Cressey’s research: “Trusted persons become trust violators when they perceive themselves as having a financial problem which is “nonsharable,” are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted fund or property.”

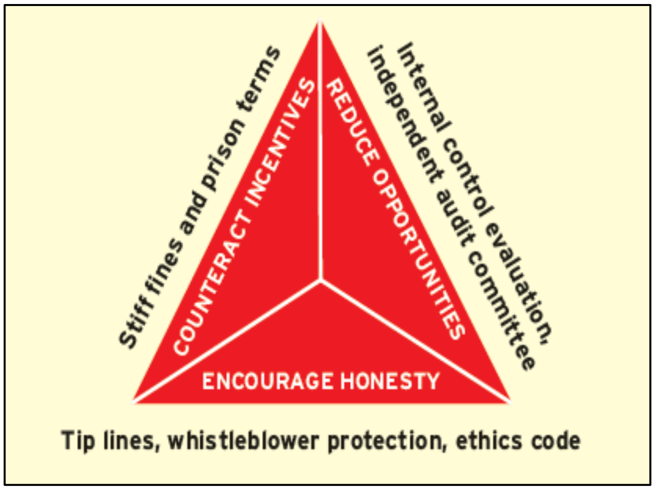
This fancy language essentially means that people who are experiencing severe financial problems about which they are embarrassed (or for other reasons cannot discuss with others) find ways to commit fraud – thinking that they will not get caught – while convincing themselves that they are doing nothing wrong.

Eventually, Cressey’s findings came to be summed up in what is now widely referred to as the Fraud “Triangle”. *The three components of the Fraud “Triangle” are* Pressure, Opportunity, and Rationalization.

From Phillips Libby Libby Ch. 5, 6th



The Fraud Triangle


Stiff fines and prison terms
COUNTERACT INCENTIVES
REDUCE OPPORTUNITIES
Internal control evaluation, independent audit committee
ENCOURAGE HONESTY
Tip lines, whistleblower protection, ethics code

Opportunity exists when an employee discovers a weakness in the organization’s anti-fraud controls. Such a weakness might exist, for example, if a procurement employee is able to set up a phony vendor and have fraudulent invoices paid and mailed to an address that he or she controls.

Pressure in the context of Cressey's Fraud "Triangle" relates primarily to financial difficulties, such as large amounts of credit card debt, an overwhelming burden of unpaid medical bills, large gambling debts, extended unemployment, substance addiction or similar financial difficulties.

Rationalization – the third element of the Fraud "Triangle" – is a psychological process whereby individuals who have committed fraud (or are about to) convince themselves that the act is either not wrong or that even if it *is* wrong, it will be corrected because they will eventually return the money.

Examples are employees may feel overworked, underpaid (or are unhappy with their raise), unfairly treated, or underappreciated. These feelings can breed employee resentment or motivation for revenge. Strict company budgeting or general economic uncertainty can exacerbate these feelings.

Another, often more damaging form of rationalization occurs when employees justify the fraud by taking the attitude that they *deserve* the stolen money – because the company was unfair in denying them a raise or promotion, or that some other form of mistreatment made them "victims."

Cressey's theory teaches that when all three of these elements are in place in an individual's life, he or she is likely to commit fraud (or already has).

CASE STUDY

How Arson Tipped Off Investigators to Massive Financial Statement Fraud

Herman Jacobowitz, former CEO of the now-bankrupt Allou Healthcare Inc., pleaded guilty to conspiracy to commit bank fraud, securities fraud, mail fraud, and filing a false annual report with the Securities and Exchange Commission (SEC) in connection with the multimillion-dollar looting of his pharmaceuticals, health, and beauty products distribution company.

In addition, Herman's brother Jacob, Allou's former executive vice president, pleaded guilty to filing a false annual report with the SEC, while another brother, Aaron, who ran several Allou-controlled shell companies, pleaded guilty to money laundering. The guilty pleas relate to charges involving what prosecutors called "a staggering, decade-long bank fraud and securities fraud scheme," involving hundreds of millions of dollars of phony sales and inflated inventory that ultimately drove the company into bankruptcy.

Prosecutors say that over a period of more than 10 years ending in March 2003, the Jacobowitzes fabricated financial statements by inflating sales, by falsifying invoices and reporting millions of dollars of nonexistent inventory in order to increase the amount of money Allou could borrow under lines of credit with several banks. It is estimated that Allou's lenders lost approximately $130 million through the scheme.

The frauds were facilitated in part by the fact that the terms of the revolving credit line that the banks had with Allou allowed it to borrow based on accounts receivable. Allou's executives manipulated the company's receivables records to make millions of dollars of aged receivables appear current.

In fiscal years 2002 and 2003 alone, some $4 million of aged receivables were falsely included among the company's total $121 million in current receivables.

Because the banks allowed Allou to borrow up to 85 percent of current receivables, the company was able to fraudulently borrow approximately $3.4 million in additional funds in each of these two fiscal years.

According to court documents, for one nine-month period in 2002, the company reported revenues of $471 million, of which $158 million was represented by falsified invoices. At around the same time, the company falsely reported $60 million in nonexistent inventory.

While the company was misrepresenting its financial condition and drawing down tens of millions of dollars from bank lines of credit, much of the "borrowed" cash was being siphoned off to companies controlled by the Jacobowitz family. Between January 2002 and March 2003 alone, approximately $180 million was siphoned off to shell corporations owned by the Jacobowitz family.

A fire at an Allou warehouse in Brooklyn led to charges of bribery and insurance fraud. As a result of the fire, Allou included an insurance claim of $87 million in its third-quarter 10-Q for fiscal year 2003.

Suspicions were raised because investigators believed the amount of claimed inventory loss was overstated. Following an investigation, the fire was deemed to have been the result of arson, and Allou's insurance carriers withheld payment on the claim.

Prosecutors claim that Herman and Aaron Jacobowitz offered $100,000 to bribe an unidentified insurance official to obtain a falsified report classifying the blaze as accidental. Ultimately, $50,000 was handed to an undercover fire marshal who was working for the prosecution. Allou filed for bankruptcy in April 2003.

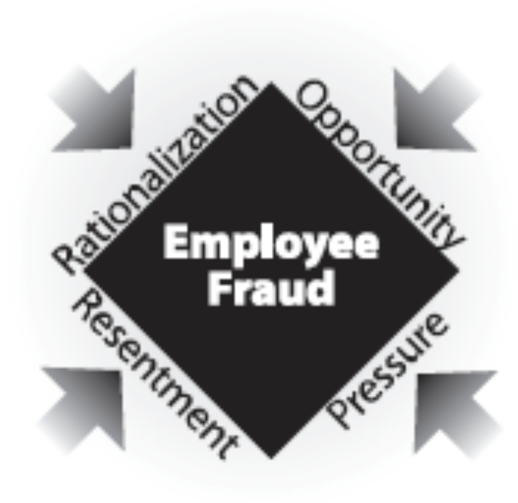
A Fraud Diamond?

The transformation of Wall Street from uncontested standard bearer of international financial integrity to hotbed of numbers-chasing mayhem in the years leading up to the financial meltdown of 2008, reveals a fourth side to the Fraud "Triangle."

It cannot be denied that in the period from 1999 until the onset of the financial crisis in mid-2008, widespread lust for money became a root cause of the debacle.

The cycle fueled by Wall Street securitization of billions of dollars of fraudulently processed and default-prone loans that generated massive commission payouts and bonuses for everyone from top Wall Street executives to Main Street subprime mortgage brokers brought a wave of avarice over the entire financial system, ultimately dooming it to its history-making crash.

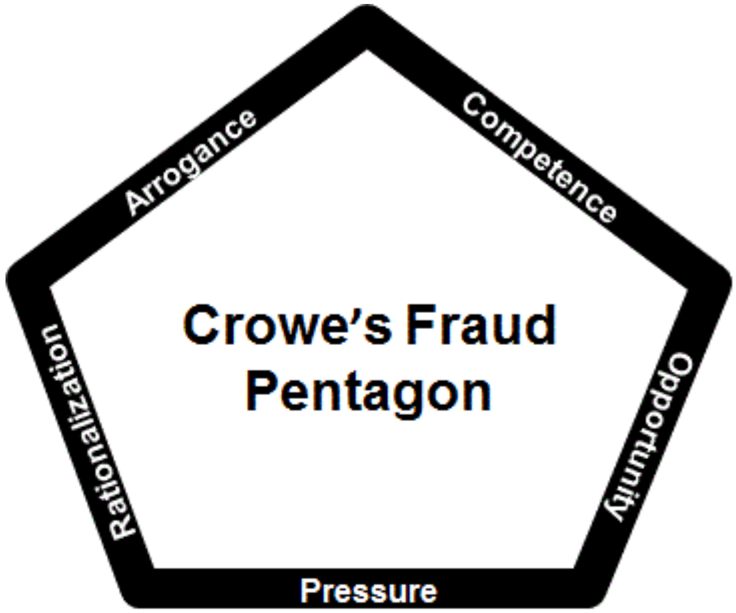
By the mid-2000s, the Fraud "Triangle," as it applied to the financial services industry, had morphed into a Fraud Diamond with *personal greed* forming the fourth side and creating new characteristics of the already deeply engrained fraud problem in the financial services industry.



G
R
E
E
D

Crowe Horwath’s Fraud Pentagon

More recently, Crowe Howath LLP expanded the fraud model to five elements, adding arrogance and competence to the fraud triangle. Frauds of this nature involve those perpetuated by higher-level employees such as middle management, CEOs, and CFOs.



They define **arrogance**, or lack of conscience, as an attitude of superiority and entitlement or greed on the part of a person who believes that internal controls simply do not personally apply.

Competence is an employee’s ability to override internal controls, develop a sophisticated concealment strategy, and to control the social situation to his or her advantage by selling it to others.

COSO Framework - Fraud

Management is responsible for assessing fraud risk and developing and implementing controls for fraud. Internal controls have a significant impact on fraud prevention and detection. The Association of Certified Fraud Examiners, in 2014, identified the anti-fraud controls most successful in reducing fraud (highest to fifth highest).

- Data monitoring
- Employee support programs
- Management review
- Internal audits both scheduled and unscheduled
- Fraud report hotline

COSO principle 8 has four focus points when assessing fraud risk.

1. Management and the Board Have an Awareness of How Fraud Can Occur and Considers Various Types of Fraud – management's fraud assessment considers fraudulent reporting, possible asset losses, and corruption resulting from various ways that fraud and misconduct may occur.
   - They consider the potential for fraud in the following areas:
     - Fraudulent financial reporting
     - Fraudulent non-financial reporting
     - Misappropriation of assets
     - Illegal acts
   - As part of the risk assessment process, management identifies various fraud possibilities, considering:
     - Management bias
     - Degree of estimates and judgments in external reporting
     - Fraud schemes and scenarios common in the industry
     - Geographic regions
     - Incentives
     - Technology and management's ability to manipulate information
     - Unusual or complex transactions
     - Vulnerability to management override

2. Management Assesses Incentives and Pressures – management's fraud risk assessment considers incentives and pressures.

    – Management reviews the entity's incentives structure to identify incentives that may be too strong and become pressured to commit fraud. This review is performed in the context of opportunities, attitudes, and rationalizations that may allow or support fraud related to each incentive.

3. Management Assesses Opportunities for Fraud to Occur – the fraud risk assessment considers opportunities for unauthorized asset acquisition, use, or disposal; altering the organization's reporting records, or committing other inappropriate acts.

    – Opportunity refers to the ability to acquire, use, or dispose of assets, which may be accompanied by altering the entity's records.

    – The likelihood of loss of assets or fraudulent external reporting increases when there is:

        ▪ A complex or unstable organizational structure

    – High employee turnover, especially in accounting, operations, risk management, internal audit or technology

        ▪ Ineffectively designed or poorly executed controls

        ▪ Ineffective technology systems

4. Management Assesses Attitudes and Rationalizations

    – Attitudes and rationalizations by individuals engaging in or justifying inappropriate actions may include:

        ▪ Considers it "borrowing," intends to repay

    – Believes entity "owes" him something because of some form of job dissatisfaction

        ▪ Doesn't understand or care about consequences

        ▪ Doesn't understand or care about accepted ideas of decency and trust

EXAMPLE

Assessing Fraud Risk

Miriam Watson is Chief Compliance Officer at Pets R Us Supply Company. During her annual fraud risk assessment, Miriam interviews management at all of Pets R Us' locations about the state of fraud issues. The risk assessment continues with her review of inventory and shrinkage methodology, whistleblower reports, and historical fraud activities. She also looks at the number of manual versus automated journal entries and the number of entries that are made late due to subjective estimates, interviews HR personnel, and reviews staff files. Applying her historical knowledge to this information, she develops a preliminary assessment of the current fraud risk situation, including the attitude of local management toward fraud tolerance.

After completing her assessment, Ms. Watson submits her report to the audit committee.

Principle 9. The Organization Identifies and Assesses Changes That Could Significantly Impact the System of Internal Control

This principle is new for COSO's 2013 Framework update and formally includes identifying and assessing significant business conditions changes. Change is always present, especially in today's increasingly-dynamic, globally-complex, technology-enabled business environment.

When reviewing internal control effectiveness, too often the default control position becomes "same as last year." Auditors, too, fall into this trap. In reality, the longer a process or system is in place, the greater the likelihood that it will deteriorate. As a result, this necessitates a fresh risk reexamination. Management must reassess risk as business conditions change.

COSO guidance is for management to document, before determining whether a certain control exists, how it achieves its stated objectives. COSO intends for this to be an unstructured approach to provoke thought, as opposed to a structured approach such as using checklists. At first this may create what appears to be many potential controls which is inefficient; however, the risk assessment stage is not the time to focus on control efficiency.

After identifying changes, management needs to analyze how each change may challenge or support the organization's strategic direction and operational objectives. This analysis requires documentation the identified changes as well as evidence management used in its risk assessment of each change which can clarify management's assessment judgment perspective.

Change that impacts business operations and, in turn, impacts internal controls can originate from many directions. COSO principle 9 has three focus points when assessing changes that could impact the internal control system.

1. Management Assesses Changes in the External Environment

    - Management considers changes that have taken place or may occur shortly in:
        - Regulatory environment

            - Economic cycles
            - Political environment
            - Physical environment
            - Marketplace evolution

        - Competitor dynamics
        - Information technology advances
        - Social and demographic trends

2. Management Assesses Changes in the Business Model
    - Management considers changes in the business model, such as:
        - New or dramatically altered business lines
        - Altered service delivery system
        - Significant acquisitions and divestitures
        - Foreign operations, especially expansion or acquisition
        - Rapid or declining growth
        - New technology
3. Management Assesses Changes in Leadership
    - Management considers significant personnel changes
        - Management turnover and succession
        - Accounting and finance department turnover
    - A new member of senior management may impact
        - Not understand the entity's culture
        - Introduce a different management or operating philosophy
        - Change strategy
        - Focus on performance to the exclusion of control-related activities
    - Organizational structure

Risk Assessment Process

The focus risk of fraud and error is not new but it is one of the points highlighted as changed in the 2013 framework. When management assesses the risk of fraud or error, the various internal and external factors noted above are considered. Then they are evaluated against the likelihood that they could occur and the magnitude if they did.

EXAMPLE

Management of a social service organization wanted to evaluate the risk related to the entity's funding sources and bring the risks to the attention of the board of directors. Some of the risk factors were:

- Size of the program and growth/downsizing
- Nature of funding and types (federal, state, local)
- Nature of transactions (solicited donations, unsolicited donations, fee for service income using sliding scale, government rates for service)
- Quality and timeliness of reporting (program and accounting)
- Quality of management and turnover (finance and program)
- Results of prior year's internal, external and statutory audits
- Perception of political, social and economic environment
- Oversight provided by funding sources and by management and the board
- The CFO prepared the first set of risks and then used that information to go to others within the organization including the board members to solicit input as to the likelihood that the risk could occur and the magnitude if it did. These three items were identified as the most likely to have a material effect on the entity.
- Uncertainty related to government funding for programs
- Lack of diversity of funding sources, dependence on federal money
- Decreased reimbursement from state agencies for services
- Bequests are not predictable

Based on this assessment, the board and management conducted a brainstorming session on how to mitigate these risks.

Risk assessments can be improved using benchmarking techniques and analytics. Some financial benchmarks that could be used might be financial such as sales (per location), gross margin (total and by significant product), payroll in total, other significant inputs in total, days in accounts receivable, inventory turnover, days in accounts payable, level of reserves, current ratio, and debt service coverage.

Statistics such as units sold, units produced, inventory units on hand, full-time equivalent employees can be used to tease the volume out of the changes in financial statement accounts.

Management should perform a vertical analysis that compares the expense categories as a percentage of revenue. This will help to evaluate the level of expenses considering changes in volume due to sales. The horizontal review should be conducted as well to see the changes overall. In addition, a comparison of budget to actual is a meaningful and helpful review procedure.

Diagnostics could be run using data extraction software to help understand risk which might include:

- Vendors with the same addresses as employees
- Vendors with P.O. boxes
- Duplicate payments
- Cash levels from week to week (focus on cash received)
- Journal entries to examine (evaluate those that are not routine, especially as it relates to writing off assets)

Depending on the industry, there may be other types of queries that are meaningful.

Following are examples of approaches that small to mid-size entities can use to implement controls dealing with the client's risk assessment process along with documentation that they should consider to evidence that control's implementation. Adequate documentation makes it easier for the auditor to perform risk assessment procedures. When the entity does not provide adequate documentary evidence, the auditor is challenged to accomplish the observation and inspection. Since many smaller entities do not have formal risk assessment processes, the only procedures the auditor may be able to perform are corroborative inquiry.

Note that the examples listed below are options for the entity. Not every entity will implement every control. In fact, smaller companies may not have formal risk assessments. The auditor's task is to determine that the risk assessment function is appropriately designed as a whole, not that every possible control is implemented.

EXAMPLE APPROACHES THAT SMALL TO MID-SIZE ENTITIES CAN USE

Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to financial reporting objectives

- Management adopts accounting policies that are appropriate for the entity and consistent with GAAP (or an OCBOA).
- Entity objectives are established, communicated, and monitored. The key elements of the entity's strategic plan are communicated throughout the entity.
- Financial reporting objectives align with the requirements of GAAP (or an OCBOA).
- Management identifies risks related to laws or regulations that may affect financial reporting.
- The accounting department has a process in place to identify and address changes in GAAP (or an OCBOA).

Principle 7: The entity identifies risks to achieving its objectives and analyzes risks to determine how the risks should be managed.

- Mechanisms are in place to identify risks potentially affecting the achievement of the entity's objectives, including (1) changes in operating, economic, and regulatory environments; (2) participating in new programs or activities; (3) offering new services; (4) communication at various levels of management; (5) application processes; and (6) information technology infrastructure and processes.

- Periodic reviews are performed to, among other things, anticipate and identify routine events or activities that may affect the entity's ability to achieve its objectives.
- Risks potentially affecting the achievement of financial reporting objectives are identified.
- Management identifies risks related to laws or regulations that may affect financial reporting.
- Risks related to the ability of an employee to initiate and process unauthorized transactions are appropriately identified.
- Management identifies all significant relationships including service providers, suppliers, donors, volunteers, creditors, etc.
- Periodic risk assessments are reviewed by management.
- Management develops plans to mitigate significant identified risks, including designing and implementing appropriate controls.

Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of financial reporting objectives.

- Fraud risk assessments are an integral part of the risk identification process.
- The entity's assessment of fraud risk considers incentives and pressures, attitudes, and rationalizations as well as the opportunity to commit fraud.
- The entity's assessment of fraud risk considers risk factors relevant to its activities and to the geographic region in which it operates.
- The entity assesses the potential for fraud in high-risk areas, including revenue recognition, management override, accounting estimates, and nonstandard journal entries.
- Those charged with governance (if separate from management) understand and exercise oversight of the entity's fraud risk assessment process.

Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

- Management has established triggers for reassessment of risks as changes occur that may impact financial reporting objectives (e.g., new accounting principles, non-routine transactions, new products, etc.).
- Management communicates the risk assessment and changes in the business environment to all appropriate employees.
- Budgets/forecasts are updated during the year to reflect changes in the entity's activities.

Given the extent of risk in today's business environment and the prevalence of fraud, it is important for management to consider performing a more formal risk assessment to include the risk of fraud or error. For each financial statement line item, the entity would assess the quantitative and qualitative aspects involved.

- **Impact on the financial statements (quantitative)** – this would be as a percentage of the total; that is, for balance sheet accounts, a percentage of total assets; for income statement accounts, a percentage of revenue.

  - A manufacturing company looks at the impact of changes in the price of inputs which have increased over the year to determine the risk and relates the magnitude to cost of sales and inventory accounts.

- **Account characteristics** – these would be quantitative and qualitative assessments considering the volume of transactions processed through the account, accounting complexity, judgment required and regulations.

  - A small city government that recently annexed a portion of a previously unincorporated county assesses the impact of the change in volume to the information technology presently used.

- **Business process characteristics** – complexity of the process, centralization of the process, presence of external relationships within the process (vendors, customers, creditors, other related parties)

  - A chain of retail stores with locations in several cities assesses the risk of a shared services arrangement to improve economies of scale.

- **Fraud risk** – assess each account for the potential for fraudulent financial reporting or misappropriation of assets

  - A not-for-profit organization assesses the risk of misappropriation of assets in light of the organization's characteristics – risk of management override, lack of segregation of duties and a significant amount of revenue received in the form of cash.

- **External factors** – consider competition, market forces, industry conditions, regulatory and political environment and changes in technology, supply sources, customer demands or creditor requirements.

- **Entity level factors** – numbers of personnel, qualifications, disruptions in information systems processing, changes in personnel or responsibilities, employee access to assets, and segregation of duties.

  - A small family owned company has inexperienced accounting staff. There is also a lack of segregation of duties. The owners performed a "risk assessment" to determine how to best handle the risk associated with error as well as fraud.

Documentation could take the form of a rating for each risk identified from 1-5 (low to high). Risks could be prioritized as to their likelihood of occurrence and the magnitude of the misstatement that could result if they did occur.

Auditor's Risk Assessment Procedures Related to the Risk Assessment Process

The auditor is required to perform risk assessment procedures on the client's risk assessment process. AU-C 315 provides guidance on the extent of understanding of the risk assessment process that is required.

> "The auditor should obtain sufficient knowledge of the entity's risk assessment process to understand how management considers risks relevant to financial reporting objectives and decides about actions to address those risks."

Since many smaller entities do not have a formal risk assessment process, the auditor will want to focus on management's processes and decisions, as follows:

- What process does management use to identify business risks relevant to financial reporting?
- How does management evaluate and prioritize risks?
- What process is used to estimate the likelihood of their occurrence and the magnitude of the impact on the financial statements if they did?
- How does management decide what actions to take to manage risks?

AU-C 315 acknowledges that most smaller entities do not have a formal risk assessment process and states that, in this case, the auditor should discuss with management and those charged with governance how they identify and address risks to the business. This can be accomplished in the form of a paragraph. However, with the new focus by the COSO on the risk assessment process, the auditor should consider whether the procedures performed are sufficient.

EXAMPLE

The entity does not document a formal risk assessment process. Based on my discussions with management, it appears that risks are adequately evaluated by the entity. The President reviews the financial statements and performs analytical review on the statements monthly. In addition, she discusses risk with her attorney and members of her family who sit on the board. Management believes that the fraud programs and controls are effective and would prevent or detect fraud.

NOTES

Unit 7

Control Activities

LEARNING OBJECTIVES

After completing this unit, participants will be able to:

☐ Explain what elements make up a financial reporting system

☐ Use the knowledge of the financial reporting system to assess financial reporting risk

☐ Develop control activities to mitigate the identified risks

OVERVIEW OF FINANCIAL REPORTING PROCESS AND SYSTEM

This section begins with an overview of the financial reporting process and system. Next it examines controls over accounting transactions and accounting processes.

Control activities predate COSO's 1992 Internal Control Framework. Thus, accountants are most familiar with developing, implementing, and testing these transaction controls because we have been using them for decades.

The previous section covered risk assessment which is the starting point for understanding **what controls should be** developed and implemented. The identified risks determine what controls are needed. Control activities, discussed in this section, need must link with the financial reporting risks identified in the risk assessment stage.

FINANCIAL REPORTING SYSTEM AND PROCESS

The financial reporting system encompasses several different elements:

- Accounting procedures for transaction initiation, authorization, recording, processing and reporting in financial statements
- Accounting procedures for adjusting entries

- Accounting records that support the information and specific accounts in the financial statements that are subject to accounting procedures. An example is subsidiary ledgers transferring information to the general ledger.

- Classes of transactions and account balances that are significant to the entity's operations

- Procedures used to capture and process non-routine, non-systematic transactions

- The financial reporting process for preparing the entity's financial statements. This includes the closing process, combining or consolidating entities, evaluating significant accounting estimates and disclosures.

The financial reporting system can include manual, as well as automated electronic processes. Automated electronic processes generally still have manual components. An example would be a manual review of exception or other reports. The financial reporting system can, and many times does, include electronic tools such as excel spreadsheets, where information is entered into the general ledger by journal entry. In addition, information that it outsourced to other service providers is still part of the financial reporting process, as management must take responsibility for it and include it in the financial statements.

It is important for management to have a complete documentation and understanding of the financial reporting process and system to ensure that internal controls are present, no matter where the transactions are originally recorded.

One effective way to document the financial reporting system is to create a chart that illustrates how information from various systems, spreadsheets, and external sources (i.e., service bureaus) is recorded in the general ledger. A tool such as the one below could be used to go through the financial statements to:

- Identify all significant account balances and classes of transactions

- Identify how the transactions in those accounts are entered into the general ledger

- Some transactions may be input directly from

  - calculations or accumulation of information on spreadsheets

  - documents received from third-party processors

  - system modules directly interfaced with the general ledger

- Be aware that some financial statement information may never transact through the general ledger. Therefore, it is important to understand "topside" entry recording.

Cycle	Significant?	Outsourced? Spreadsheet / Interface with GL?
Cash – Part of the Cash Receipts / Cash Disbursements and Payroll Cycles Assertions ■ Existence ■ Completeness ■ Rights and obligations ■ Allocation (note that valuation is not an assertion for cash)	Yes	Interface with GL
Accounts Receivable / Revenue / Orders and Shipments / Billings / Returns / Collections Assertions ■ Occurrence ■ Completeness ■ Accuracy ■ Cutoff ■ Classification	Yes	Restricted contributions are maintained on a spreadsheet Minimal contributions taken over the internet
Inventories / Cost of Sales Purchase Orders / Receiving / Compilation and Pricing of Inventory / Obsolescence Evaluation Assertions ■ Existence ■ Completeness ■ Rights and obligations ■ Valuation and allocation	Yes	Inventory summarized on a spreadsheet at year-end and adjustment made to reflect change in asset balance
Prepaid Expenses Additions / Amortization / Impairment Evaluation Assertions ■ Existence ■ Completeness ■ Rights and obligations ■ Valuation and allocation	No	N/A

Cycle	**Significant?**	**Outsourced? Spreadsheet / Interface with GL?**
Property / Additions / Sales / Amortization / Depreciation Assertions ■ Existence ■ Completeness ■ Rights and obligations ■ Valuation and allocation	Yes	Property is keyed into firm accounting software to compute depreciation and make entry to adjust accumulated depreciation
Other Assets Additions / Amortization / Impairment Evaluation Assertions ■ Existence ■ Completeness ■ Rights and obligations ■ Valuation and allocation	No	N/A
Accounts Payable / Purchasing / Receiving / Expenses Assertions ■ Existence ■ Completeness ■ Rights and obligations ■ Valuation and allocation	Yes	Interface with GL
Accrued Expenses Purchasing / Receiving / Expenses Assertions ■ Existence ■ Completeness ■ Rights and obligations ■ Valuation and allocation	No	N/A
Deferred Revenue / Revenue Recognition Assertions ■ Existence ■ Completeness ■ Rights and obligations	Yes	Deferred revenue is summarized on a spreadsheet at year-end and adjustment made to reflect change in liability balance

Cycle	Significant?	Outsourced? Spreadsheet / Interface with GL?
■ Valuation and allocation		
Mortgages and Notes Payable / Borrowings / Repayments / Interest / Evaluation of Covenants <u>Assertions</u> ■ Existence ■ Completeness ■ Rights and obligations ■ Valuation and allocation	Yes	Interface with GL
Equity / Stock Issuance / Purchase of Treasury Stock / Dividend Payments <u>Assertions</u> ■ Occurrence ■ Completeness ■ Accuracy ■ Cutoff ■ Classification	Yes	Interface with GL
Payroll / Accrued Payroll / Expenses / Payroll Taxes / Employee Benefits <u>Assertions</u> ■ Occurrence ■ Completeness ■ Accuracy ■ Cutoff ■ Classification	Yes	Payroll is outsourced with journal entry made to record activity in GL

EXAMPLE

The accounting manager of an industrial cleaning company was preparing to go through an initial audit. She knew the auditors would be evaluating the company's internal control. The auditors asked her to identify the significant systems that process transactions. She listed the following:

- Cash receipts – cash receipts module directly interfaced with the general ledger
- Cash disbursements – cash disbursements module directly interfaced with the general ledger
- Payroll – outsourced to a third-party service provider

The internal auditor looked at the information and asked her to look at each account on the balance sheet and income statement and consider how the transactions were processed. She took another look and identified two more:

- Investments – outsourced to a third-party service provider
- Inventory – maintained on a spreadsheet, journal entry made to record activity in the general ledger

Risk Assessment Procedures for the Financial Reporting System and Processes

Management is required to assess financial reporting risk. It is important to distinguish between the financial reporting system that includes all of the processes described above and the financial reporting process that includes how information is taken from the general ledger and other sources and turned into financial statements.

Controls over financial reporting are not independent of IT. Information Technology (IT) quality has a large impact on the organization achieving its financial reporting objectives. IT also affects how transactions are initiated, authorized, recorded, processed, and reported. Even highly-automated electronic systems, however, have some manual processes.

Manual process controls take the form of approvals, activity reviews, and reconciliations. Manual action exists for exceptions to these activities and automated system-generated exception reports. An example of automated electronic system is purchase orders, receiving documents, invoices received replacing paper documents with an automated three-way match.

Financial reporting process risk assessment over presentation and disclosure are:

- Occurrence and rights and obligations – disclosed events and transactions have occurred and pertain to the entity
- Completeness – all disclosures that should have been included in the financial statements have been included
- Classification and understandability – financial information is appropriately presented and described and disclosures are clearly expressed
- Accuracy and valuation – financial and other information are disclosed fairly and at appropriate amounts

Management documents automated and manual processes used to prepare financial statements and related disclosures so they can assess how misstatements might occur. Financial reporting process and management’s objectives follow.

Financial Reporting Processes and Control Objectives

Control Objectives	**Financial Reporting Processes**
1. Management is **aware** of the need for the fair presentation of the financial statements including: ■ Selection of accounting pronouncements ■ Key accounting estimates ■ Evaluation of assets for impairment ■ Presentation and disclosure The company has a process in place to **gather reliable information** for decision making processes Management **uses the information to make decisions** affecting the financial reporting processes Management ensures that **high level journal entries or management overrides have the appropriate approval**, which may be that of the board of directors	■ Procedures to enter transaction totals in the general ledger. Recording non-routine, non-systematic entries, post-closing adjustments, consolidating entries and reclassifications ■ Procedures used to initiate, authorize, record and process journal entries in GL ■ Procedures for drafting financial statements and disclosures, including consolidation ■ Selection and application of accounting principles ■ Consideration of asset valuation ■ Consideration of contingent liabilities, consolidation issues and off balance sheet financing ■ Preparation of significant accounting estimates

Following is a description of possible internal controls that would support management's objectives concerning the preparation of complete and accurate financial statements.

Control Objectives	**Financial Reporting Processes**
Management is **aware** of the need for the fair presentation of the financial statements including: ■ Selection of accounting pronouncements (GAAP) ■ Key accounting estimates ■ Evaluation of assets for impairment ■ Presentation and disclosure	Senior management, the board of directors and the audit committee consist of individuals with the necessary knowledge, skills, and experience, including those with financial expertise. Senior management, the board of directors, and the audit committee take the necessary steps to remain current on industry developments, changes in the regulatory environment, and changes to accounting and reporting requirements. Senior management consults with internal and external experts early in the process of structuring transactions.
The entity has a process in place to **gather reliable information** for decision making processes	Management obtains and considers information from reliable sources to prepare its accounting estimates or identify and record non-routine events such as impairment of assets. For example, workmen's

	compensation claims data is provided by outside claims processor. Management assembles and prepares the appropriate evidence to support non-routine journal entries.
Management **uses the information to make decisions** affecting the financial reporting processes	Management has a formal process for closing the books and preparing financial statements which includes all the appropriate closing and consolidating entries, as well as the preparation of the appropriate disclosures.
Management ensures **that high-level journal entries or management overrides have the appropriate approval**, which may be that of the board of directors	Management reviews significant estimates and support for all non-routine entries. The board of directors reviews, approves and, assesses the quality of the entity's accounting principles. Accounting policies are documented and communicated to all personnel that need the information. A specific member of management reviews the financial statements to assess their fair presentation.

An **owner's** involvement in the organization's operations (e.g., customer relations, bank relationships, etc.) is not the same as active involvement in the financial reporting process. However, if the owner is truly actively involved in the financial reporting process, the auditor should recognize that this is both a control and a risk regarding management override.

COSO FRAMEWORK PRINCIPLES – CONTROL ACTIVITIES

Control activities are management actions established through policies and procedures. They help to ensure that transactions are processed, completely, accurately, and timely as well as prevent or detect and correct errors and fraud.

Control activities are performed at all levels of the entity and include activities manually performed by employees and automated through systems. Manual control examples are authorizations, approvals, verifications, reconciliations, and business performance reviews. Automated controls are included within information technology applications that processes transactions. Controls can be present at the entity or at third party service providers.

The COSO Framework includes management considering whether the identified risks surrounding its stated business and financial reporting objectives have been mitigated by controls that management designed and implemented. The framework also includes information technology automated financial reporting processes and systems. Finally, it includes transaction controls including the financial statement close process which has management judgment for estimates and valuations.

This section addresses the three COSO principles under the Control Activities:

Principle 10 – Control activities that mitigate risks

Principle 11 – General control activities over information technology

Principle 12 – Policies and procedures

Principle 10. The Organization Selects and Develops Control Activities That Contribute to the Mitigation of Risks to the Achievement of Objectives to Acceptable Levels

COSO principle 10 has six focus points when assessing changes that could impact the internal control system.

1. Management Integrates Control with Risk Assessments Performed

   – Control activities support all components of internal control, but are particularly aligned with the risk assessment component. Along with assessing risks, management identifies and puts into effect actions needed to carry out specific risk responses.

2. Management Considers Entity-Specific Factors

   – Since each entity has its own set of objectives and implementation approaches, there will be differences in objectives, risk, risk responses, and related control activities.

     Generic control checklists will rarely be effective because every organization faces different risks with different levels of impact magnitude and occurrence likelihood. Industry-based risk checklists may provide more relevant ideas, because industry players share broad risks, such as regulation and technology. However, even within an industry, individual organizations have unique risk profiles resulting from different business models, strategies, policies & procedures, capital structure, geographical locations, etc.

   – Management considers the many entity-specific factors that can impact the control activities needed such as:

     ▪ Environment and complexity

     ▪ Nature and scope of operations, both physically and logically

     ▪ Degree of regulation

     ▪ Multinational operation

     ▪ Diversity of operations

     ▪ Sophistication of enterprise resource planning (ERP) system

     ▪ Centralization/decentralization

    - Degree of innovation

3. Management Determines Relevant Business Processes

    - Business processes often cover many objectives and sub-objectives, each with its own set of risks and risk responses. A common way to consolidate these business process risks into a more manageable form is to group them according to information processing objectives:

        - Completeness – transactions that occur are recorded

        - Accuracy – transactions are timely recorded at the correct amount in the correct account

        - Validity – recorded transactions represent economic events that actually occurred

    - While these objectives are most often associated with financial processes and transactions, the goals of completeness, accuracy, and validity apply to any activity in any organization.

4. Management Evaluates a Mix of Control Activity Types

    - Management considers a variety of transaction control activities for its control portfolio including:

        - Authorizations and approvals

        - Verifications

        - Physical controls

        - Controls over standing data (e.g., master files)

        - Reconciliations

        - Supervisory controls

    - Management considers a mix of control activities that are preventive and detective. In doing so, management considers the precision needed from the control as well as what the control is designed to accomplish.

5. Management Considers at What Level Activities Are Applied

    - In addition to transaction-level controls, management selects and develops a mix of controls that operate more broadly and at higher levels. These are usually business performance or analytical reviews involving comparisons of different sets of operating or financial data. These relationships are analyzed, investigated, and corrective action taken.

6. Management Addresses Segregation of Duties

   – **Segregation of duties is intended to reduce the risk of error or inappropriate or fraudulent actions. Segregation generally separates responsibility for authorizing, approving, and recording transactions, and handling the related asset. In small entities, ideal segregation may not be practical, cost effective or feasible, and alternative control activities must be designed.**

EXAMPLE

Using Alternative Control Activities when Access to Purchasing Transactions Are Not Segregated

ArtStone Artifacts is an importer and distributor of decorative stone products from around the world. Two staff members in purchasing are each authorized to prepare, authorize, and issue purchase orders up to $4,000. No one reviews these orders, so errors or fraud could result in valuation errors, obsolescence or shortages. To reduce these risks, management has:

- An inventory clerk track inventory levels
- An inventory receiving clerk report unusual inventory movement, such as excessive purchases that could lead to obsolescence
- A payables clerk match invoices to receiving reports and purchase orders to help detect diverted shipments
- A controller review purchase price exception reports over 10% above usual cost

EXAMPLE

Evaluating Preventive versus Detective Control Activities

Rocky Mountain School for the Blind, as part of its controls review, evaluates the mix of preventive versus detective controls, and finds a high proportion of detectives. This causes transaction processing to be slow, labor intensive and error prone, because much time is spent fixing errors from earlier in processing. Management decides to implement additional preventive controls, such as automated checks and data verification, and review and approval controls at transaction initiation. These changes are intended to reduce the number of errors that need to be detected and fixed later.

EXAMPLE

Establishing Policies and Procedures

A national religious education association has a policy that all payments must be authorized before disbursement, using an authorization approval matrix.

Policy provides specific limits on authority for approval of over-budget expenditures:

- Board of directors: $50,000 up
- CEO: Up to $50,000
- VP: Up to $10,000
- Staff directors and managers: Up to $2,500
- Supervisors: Up to $500

All purchases require a purchase order and invoice, except investments which are covered by the board-authorized investment policy.

Control activities consist of control activities and the application controls within the information and communication category. Information technology application controls will not be discussed here as they are beyond the scope of this course. **Much of this section concentrates on manual controls that are typically found in small to mid-size entities.**

Control activities are the policies and procedures that help ensure that management's directives are carried out. Broadly, there are four categories of control activities:

- **Authorization controls** – these relate to the initiation of transactions. For example, invoices should be authorized by an employee with the appropriate level of responsibility prior to payment.
- **Safeguarding assets** – these controls relate to the protection of assets from damage or theft. For example, inventory should be properly stored with limited access.
- **Asset accountability** – these controls relate to the reconciliation of detailed records to the general ledger. For example, reconciliation of accounts receivable subsidiary detail to the general ledger should be performed on a regular basis.
- **Segregation of duties** – these controls separate duties between personnel so that no one individual employee can complete a significant business transaction in its entirety. For example, an employee with access to the incoming cash receipts should not have access to the accounting records. Segregation of duties was discussed in a previous section.

Control activities can be preventive, detective, or corrective.

- Preventative controls identify errors on the front end as they occur and prevent them from being recorded in the financial reporting system. They are the most effective controls because they prevent errors from occurring up-front. These are active controls that are employed regularly.

  Examples are:

  - restricted access with mechanical locks to rooms
  - computer system access
  - information system password access
  - disaster recovery
  - segregation of duties
  - employee background checks

- transaction authorization

- Detective controls identify and correct errors that are already transacted in the financial reporting system. They are part of checks and balances processes.

  Examples are:

  - account reconciliations
  - exception reports
  - physical inventory
  - financial statement and operations analytical review
  - internal audits
  - security cameras

- Corrective controls correct errors identified by detective controls. This includes a reporting process to supervisors for root cause analysis and implementing control improvements so the error does not reoccur. The reporting process is also necessary for employee disciplinary actions.

  Examples are:

  - accounting policies and procedures for reporting errors
  - training on technical accounting and financial reporting policies and procedures
  - employee disciplinary actions

Most control systems include all these controls primarily because it is more difficult and expensive to implement sufficient controls on the front end. The trade-off is that lower-cost detective and corrective controls result in less timely information and inefficient re-work.

Note that effective controls must be designed and implemented both to:

- Identify a misstatement
- Correct the misstatement

Examples of the various types of control activities follow:

Control Activities Examples

Top Level Reviews	**Access Controls**
■ Comparison of budget to actual, actual to prior year ■ Comparison to benchmarks or other performance indicators ■ Comparison of actual cash receipts and disbursements to expectations and follow-up on variances ■ Comparison of budgeted or expected sales to actual sales and analytical review with accounts receivable ■ Analytical review of costs of sales to sales and to inventory ■ Analytical review of expenses ■ Scanning the General Ledger for unusual activity	■ Physical access to assets, files, computer programs, accounting records ■ Comparison of periodic asset counts to control records ■ Use of a lockbox ■ Cash stored in a secure location ■ Periodic inventory counts ■ Signature plates for checks stored in a controlled place ■ Periodic counts of inventory and reconciliation ■ Periodic counts of significant property items, permanent ID tags are attached to assets
Activity Management ■ Review of bank reconciliations ■ Review of customer statements before mailing ■ Review of Accounts Receivable aging and the allowance for doubtful accounts ■ Review of reconciliations of subsidiary ledgers with General Ledger ■ Review of standard cost variances ■ Review of reconciliation of physical inventory counts with perpetual records or General Ledger control accounts	**Activity Management** ■ Review of application of overhead, direct materials and direct labor to work in process ■ Review of inventory for obsolescence ■ Review of interest and dividend income, including accretion ■ Review of classification of securities and mark to market ■ Evaluate assets for impairment **Other Control Activities** ■ Segregation of duties

EXAMPLE

Performing Control Activities in a Timely Manner

A research foundation, Wide Ocean Sea, promptly terminates general ledger access rights of employees no longer requiring it:

- When an employee is transferred, promoted, or terminated, an out-processing form is required, which includes a section indicating that deletion of system access has been initiated – supporting e-mail confirmations are also sent between finance, HR, and IT
- An information technology employee (IT) confirms to finance and human resources (HR) when access deletion is complete

- HR tracks open deletion orders and follows up with IT if deletion confirmation not received within 24 hours

EXAMPLE

Using a Risk and Controls Matrix to Map Risks to Control Activities

Fulton Agricultural Implements is a manufacturer of specialized tractor-drawn farming implements. In connection with its risk assessment process, the company has developed a decision-support matrix covering financial reporting assertions and objectives, identified risks and control activities. The matrix addresses areas such as regulatory matters, financial statement preparation, closing and consolidation processes, estimates and reserves, accruals, and general ledger procedures. Each control is addressed in enough detail to permit evaluation as to whether it could be effective in reducing the relevant risk to an acceptable level. Management also evaluates the mix of different types of controls (such as prevention vs. detection and automated vs. manual).

Following is an excerpt of one FAI control and risk process description and matrix.

Flow of the Ordering Process

Purchasing Department

1. Initiate Purchase Order
2. Update Vendor Master File
3. Update Price Master File
4. Send to AP System

AP System

1. Perform Edit and Validation
2. Update Vendor Master File
3. Update Price Master File
4. Return to Purchasing Department

Purchasing Department

1. Generate Purchase Order
2. Send to Buyer

Buyer

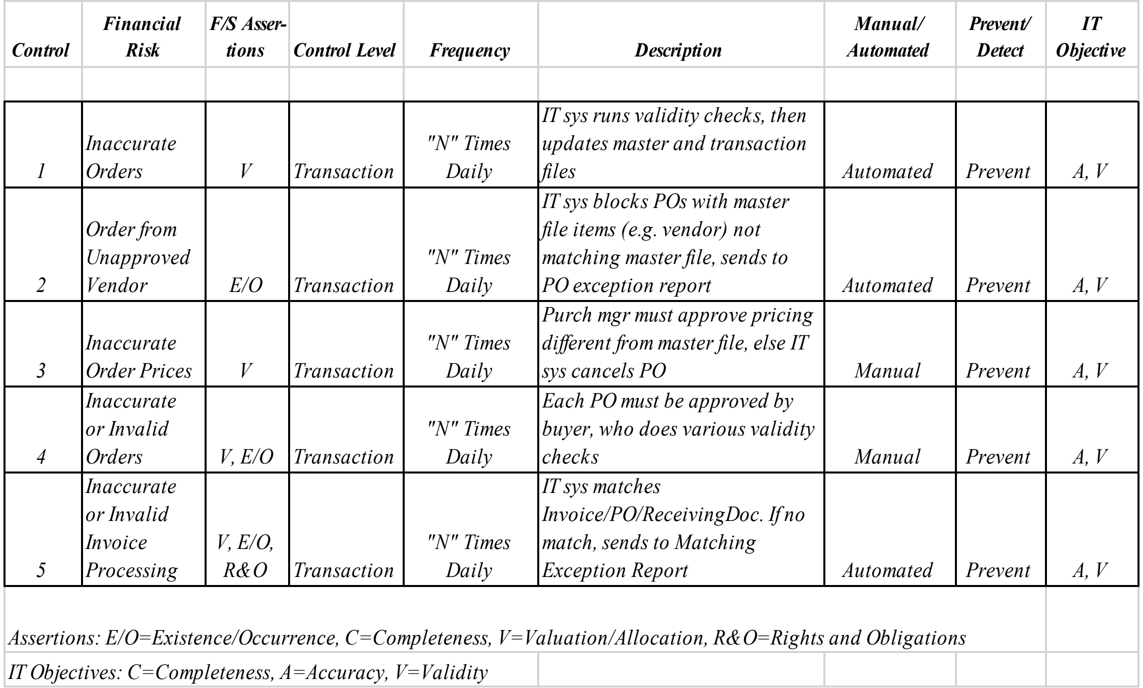
1. Approve Purchase Order
2. Send to Accounting Department

Flow of the Invoice Processing

Accounting Department

1. Receive Invoice from Vendor
2. Input Invoice
3. Update AP Ledger
4. Receive Approved Purchase Order from Buyer

5. Receive Goods Received Document from Receiving Department
6. Match Invoice / Purchase Order / Goods Received Document
7. Record Invoice
8. Update General Ledger



Control	Financial Risk	F/S Assertions	Control Level	Frequency	Description	Manual/ Automated	Prevent/ Detect	IT Objective
1	Inaccurate Orders	V	Transaction	"N" Times Daily	IT sys runs validity checks, then updates master and transaction files	Automated	Prevent	A, V
2	Order from Unapproved Vendor	E/O	Transaction	"N" Times Daily	IT sys blocks POs with master file items (e.g. vendor) not matching master file, sends to PO exception report	Automated	Prevent	A, V
3	Inaccurate Order Prices	V	Transaction	"N" Times Daily	Purch mgr must approve pricing different from master file, else IT sys cancels PO	Manual	Prevent	A, V
4	Inaccurate or Invalid Orders	V, E/O	Transaction	"N" Times Daily	Each PO must be approved by buyer, who does various validity checks	Manual	Prevent	A, V
5	Inaccurate or Invalid Invoice Processing	V, E/O, R&O	Transaction	"N" Times Daily	IT sys matches Invoice/PO/ReceivingDoc. If no match, sends to Matching Exception Report	Automated	Prevent	A, V

Assertions: E/O=Existence/Occurrence, C=Completeness, V=Valuation/Allocation, R&O=Rights and Obligations

IT Objectives: C=Completeness, A=Accuracy, V=Validity

Assertions

Management assertions are claims made by members of management regarding certain business aspects. Management assertions fall into the following three classifications. There is a fair amount of duplication in the types of assertions across the three categories; however, each assertion type is intended for a different aspect of the financial statements, with the first set related to the income statement, the second set to the balance sheet, and the third set to the accompanying disclosures.

1. Transaction-level assertions. The following five items are classified as assertions related to transactions, mostly in regard to the income statement:

   - Accuracy. The assertion is that the full amounts of all transactions were recorded, without error.

   - Classification. The assertion is that all transactions have been recorded within the correct accounts in the general ledger.

   - Completeness. The assertion is that all business events to which the company was subjected were recorded.

- Cutoff. The assertion is that all transactions were recorded within the correct reporting period.

- Occurrence. The assertion is that recorded business transactions actually took place.

2. Account balance assertions. The following four items are classified as assertions related to the ending balances in accounts, and so relate primarily to the balance sheet:

   - Completeness. The assertion is that all reported asset, liability, and equity balances have been fully reported.

   - Existence. The assertion is that all account balances exist for assets, liabilities, and equity.

   - Rights and obligations. The assertion is that the entity has the rights to the assets it owns and is obligated under its reported liabilities.

   - Valuation. The assertion is that all asset, liability, and equity balances have been recorded at their proper valuations.

3. Presentation and disclosure assertions. The following five items are classified as assertions related to the presentation of information within the financial statements, as well as the accompanying disclosures:

   - Accuracy. The assertion is that all information disclosed is in the correct amounts, and which reflect their proper values.

   - Completeness. The assertion is that all transactions that should be disclosed have been disclosed.

   - Occurrence. The assertion is that disclosed transactions have indeed occurred.

   - Rights and obligations. The assertion is that disclosed rights and obligations actually relate to the reporting entity.

   - Understandability. The assertion is that the information included in the financial statements has been appropriately presented and is clearly understandable.

Assertions are very relevant to linking assessed risks and controls in the control activities COSO principles. Assertions can be used in evaluating financial reporting risks in accounts, transactions, classification, and disclosure.

INFORMATION TECHNOLOGY

Principle 11. The Organization Selects and Develops General Control Activities over Technology to Support the Achievement of Objectives. There Are Several Points of Focus

Information technology and computerized processes increased significantly since the original COSO Framework in 1992 which had only one information technology section. As a result, COSO's 2013 revised framework includes information technology in 14 of the total 17 principles. The new framework integrates computer systems, programs, and technology-based controls throughout all 17 principles.

In contrast to 1992, all organizations today are significantly dependent on information technology programs, networks, and systems. Information technology processes and stores transactions, documentation, and accounting information as well as communicates this accounting information to management and employees who use it in performing their duties and executing their responsibilities.

Information technology controls are not only for accounting and finance systems, such as general ledger and sub-ledgers such as fixed assets. These controls also apply to operations which can impact financial reporting. For example, product quality data may impact the warranty liability accrual and customer payment data may impact the allowance for doubtful accounts.

Spreadsheet controls are especially important. Many accountants perform accounting calculations in spreadsheets out of the organization accounting and finance electronic systems. This can become more risky when an accountant downloads system data into a spreadsheet, performs calculations, and they uploads the calculated date back into the electronic system.

COSO principle 11 has four focus points about general technology controls.

1. Management Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls and Implements Effective General Controls

   The reliability of technology within business processes, including automated controls, depends on the selection, development, and deployment of general control activities over technology. These general controls help ensure that automated processing controls work properly initially, and that they continue to function properly after implementation. General controls apply to technology infrastructure, security management, and technology acquisition, development, and maintenance. They also apply to all technology, both IT and technology used in production processes.

2. Management Establishes Relevant Technology Infrastructure Control Activities

   Technology infrastructure may include computers, networks, power supplies, backup systems, software, and robotics. This infrastructure is often complex and rapidly changing. These complexities present risks that need to be understood and addressed, and management should track changes and assess and respond to new risks.

3. Management Establishes Relevant Security Management Process Control Activities

   Security management includes sub-processes and controls over whom and what has access to an entity's technology, including who has the ability to execute transactions. Security threats can come from both internal and external sources. Evaluating and responding to external threats will be more important when there is reliance on telecommunication networks and the internet.

   Internal threats may come from former or disgruntled employees, who pose unique risks. User access to technology is generally controlled by authentication controls. These controls are very important and are often the most abused by employees who may share access codes (generally passwords) and IT personnel who do not immediately shut off an employee's unneeded access to systems resulting from job change or termination.

4. Management Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities

   Technology controls vary depending on risks. Large or complex projects have greater risks, and control rigor should be sized accordingly. Use of packaged software can reduce some risks versus in-house software development. Another alternative is outsourcing, which, however, presents its own unique risks and often requires additional controls.

IT contributes significant benefits to an entity but also poses significant risks as noted below. These benefits and risks will vary with system complexity, and whether the software applications are packaged or customized.

Benefits and Risks of Information Technology to the Entity's Internal Control Structure

Benefits of Information Technology	**Risks of Information Technology**
■ Consistent application and calculation when processing large amounts of data ■ Enhanced timeliness, availability and accuracy of information ■ Aids in analysis ■ Better ability to monitor the entity's activities ■ Minimizes risk that controls will be circumvented ■ Better segregation of duties	■ Reliance on inaccurate data ■ Unauthorized access to data that could be improperly changed or destroyed, including recording fictitious transactions ■ Unauthorized changes in master files, systems or programs ■ Necessary changes to systems or programs not made ■ Inappropriate manual intervention ■ Possible loss of data or inability to access data, when needed

Understanding the entity's internal controls over information technology becomes increasingly important as technology expands into everyday workflow. Even standard-packaged software does not keep the organization from being vulnerable to fraud from outside as well as inside the organization.

Unauthorized system access is an issue in both small and large entities, which effective internal controls help to prevent or detect. Management needs information system controls, including the related business process relevant to financial reporting, for:

- Procedures used to initiate, authorize, record, process and report information in the financial statements whether automated or manual
- Related accounting records, whether electronic or manual, supporting information and specific accounts in the financial statements
- How the information system captures events and conditions, other than classes of transactions that are routinely processed
- Process used to prepare the entity's financial statements including significant accounting estimates and disclosures
- Procedures and technology such as firewalls used to safeguard the entity's data

EXAMPLE

Configuring the IT Infrastructure to Support Restricted Access and Segregation of Duties

Networks, operating systems, databases, and applications supporting financially significant processes must support restricted access to financial applications and data in conformity with organizational policy. This includes user authentication, access enforcement, and required parameters such as password format and a requirement to periodically change passwords.

Electric Boat Company has a number of financially critical applications. Recently their external audit department cited a significant deficiency for poor infrastructure security controls. Password format requirements were not consistently applied and some were below industry security standards. Electric Boat designed a four-step remediation plan:

- Rate each application on its importance to financial reporting reliability
- Specify security policies for each rating level
- Assign each application a risk rating relating to its impact on financial reporting reliability
- Implement procedures to enforce policy compliance consistent with each application's ratings

IT and Smaller Entities

Smaller entities can establish more effective internal control if they use standard packaged software rather than customizing purchased packages or custom-developing in-house software. Standard package software requires fewer controls for program change management. Packaged programs also have certain automated controls and documentation that smaller entities can rely on. This will be discussed later in this section.

Information technology control components

COSO does not give guidance on specific approaches, processes, or procedures for assessing information technology controls. Activity controls may be automated controls. Examples are using the system to record and classify financial transactions or using the system to perform the three-way match of purchase orders, invoices received, and receiver reports.

Generating and delivering system-generated reports that employees rely upon to perform their job function uses data bases and communications networks. Examples are sales reports, receivables aging, and inventory aging. This communications function also applies to management review (monitoring) controls and includes characteristics of relevant, reliable, and timely reports. Examples are financial statements, product or customer profitability, department budget variances

The COSO framework includes three components related to IT controls:

1. **Application Controls:** Application controls are built into computer programs. They are designed to provide information processing completeness and accuracy which is important to the integrity of the financial reporting process, authorization, and validity.

   They are specifically related to the classes of transactions and account balances.

   Applications may be the general ledger system and its various interfacing modules such as accounts receivable, accounts payable or payroll or non-interfacing systems such as fixed asset packages or other systems that process information that ends up in financial statements.

   Application controls can be automated when contained in the computer program or manual when performed by an individual. If the entity has an integrated ERP (enterprise resource planning) environment such as SAP, Oracle or JD Edwards, many of the application controls have already been programmed. Where the system is not quite so robust, the control objectives may be able to be satisfied by manual controls such as investigating exceptions or errors generated in processing.

   Overall control objectives of any IT application are to ensure:

   - Complete, accurate, and valid data

   - Output that is distributed to authorized users

   There are four broad types of application controls that are used to achieve the internal control objectives of the various cycles.

   - Input controls – These controls are designed to ensure that the data entered into the system is complete and accurate

   - Processing controls – These controls are designed to ensure that data is processed completely and accurately and data integrity is maintained while processing and in storage

- Output controls – These controls are designed to ensure that reports produced by the system are distributed to only authorized personnel

- Security controls – These controls ensure that data stored and processed by the application are protected from unauthorized access, modification or loss

A comprehension discussion of application controls is beyond the scope of this course. For more information, IT Control Objectives for Sarbanes-Oxley, an ISACA publication, can be found at http://www.isaca.org.

2. **General Computer Controls:** General computer controls are ensure integrity of the overall system, data, and applications. General controls provide overall information technology reliability by providing user access and security. Thus, they protect data from unauthorized changes and restrict accounting program access to protect against recording unauthorized transactions or making unauthorized accounting estimate changes. They are not related to specific applications nor to data processing.

   General computer controls are broad and include controls over overall information technology (i.e., control environment). Components include:

   - Access and security controls
   - Change management
   - Systems development
   - Systems maintenance
   - Data backup and recovery
   - Operations
   - Physical security that is related to the integrity of financial reporting processes

   Access and security are the most critical controls which include user access to applications and to data. Permissions limit user access only to the applications and data necessary to perform their job function, and include which employees are authorized to grant user access. In addition, this impacts both organization operations as well as government and industry compliance adherence.

   Access controls include user password management. Examples are disallowing common passwords (such as 12345), requiring strong passwords, requiring periodic password changes, prohibiting password sharing, and requiring physical password security (disallowing visually displaying passwords on post-it notes on the computer or workstation).

   Change controls are most critical in legacy or custom information technology systems, but also apply to purchased systems that have decision boxes to check or uncheck. Change controls are effectively a change management process encompassing initiation, approval, the change, testing and validating, user acceptance, and user training.

The danger with ineffective change controls is primarily inadvertent change, versus malicious change or change associated with fraud which are also risks.

Controls (policies) over change timing are often overlooked and can impact financial statements. For example, changes should rarely occur at critical seasonal peaks which could negatively disrupt operations, nor should changes occur at year end during the accounting close.

Controls (processes) over change include making changes in a text environment, not real-time in a production environment. This may include running parallel (old and changed) applications as a part of the validation step. Also, data back-up to avoid losing important operating and supporting documentation. In addition, changes need to be documented.

Developing new systems is closely related to change management, but is usually on a grander scale. This applies as organizations adopt new complete systems or individual system modules or upgrade versions of existing applications. The control is the process and procedures to conduct new system development without interrupting operations, accounting and finance, or data integrity.

A large risk is how the new system will work with unchanged systems because there may be operating system, hardware, or interface incompatibilities. New system development failures also result from employee capability problems of not enough time resources to perform both existing job responsibilities while developing and integrating new systems.

Systems maintenance applies to disaster recovery. This control needs to be implemented and tested before a disaster occurs. Disaster is not necessarily a complete loss from fire or flood, but also can include power and telecommunications disruption. The starting point is a risk assessment of the most vulnerable and required systems and data.

With many smaller entities, access control is often lacking and management needs to assess these risks. At a minimum, the following access controls should exist:

- Vendors can access the system only for a short period after installation
- Terminated employees no longer have access to the system
- When job responsibilities are changed, access to data is also changed

3. **End-User Computing:** End-user computing includes the use of spreadsheets and other user-developed programs (such as databases) and involves:

- Documentation of these programs
- Program security

- Back up
- Regular review for processing integrity

Most small to mid-size entities use packaged software products where the source code cannot be modified and where the software has limited connectivity to the Internet. These entities will have less need for general and application computer controls such as delete, change and incident management controls and systems development controls. Management needs system controls:

- System updates were properly installed
- New applications were tested and are running properly

Of course, there are also entities that have software programs that were developed in-house or by a local technology vendor where the entity has access to the source code. This situation requires a larger array of general computer and application controls. This program will only discuss requirements when the entity uses a packaged software product.

NOTE: If a company uses different software vendors for various applications, this will increase the risk of material misstatement.

EXAMPLE

Managing Changes to Packaged Software

Baldwin Steam Traction sells small real steam locomotives for amusement park train rides. It uses off-the-shelf general ledger software, and has developed a procedure for managing vendor software upgrades:

- Obtain a description of the upgrade, including rationale, security impact, and user interface changes
- Design a back-out plan should the upgrade fail
- Create a test plan to test that edit and validation rules work, system functions work, undesired results are prevented, and existing control activities work
- Execute the tests and document results
- Maintain a change log
- Get approval of the test results from financial and operational management and end users before going live

Approaches that Smaller Entities with Packaged Software Can Use

Following are examples of approaches that smaller entities can use to implement IT controls, along with documentation shows control implementation. These examples are options, and not every organization will require every control. The control examples that follow include automated and manual controls.

Example approaches that small to mid-size entities can use

Control	**Demonstrates**	**Entity Documentation**
The entity secures access to important IT applications, databases, operating systems and network devices: ■ Account set-up, change, and termination standards. ■ Authentication controls regarding the minimum requirements for IDs and passwords. ■ Review of restrictions on external connectivity to the system such as firewalls, Virtual Private Network (VPN) connections and dial up. ■ Access to system IDs for important applications, databases, operating systems and network devices is restricted. Approval to have an ID is obtained from the appropriate level of management and is reviewed. ■ Antivirus software is used to protect the integrity and security of the system. ■ Processes are in place to update to current versions.	Concern for the integrity of data and that transactions are not altered or deleted.	Policies and procedures.
The entity develops change and incident management processes[25] such as: ■ Significant changes to operating systems are initiated, approved, and tracked. ■ For significant upgrades to the system, all changes are tested prior to release into production. ■ If any emergency changes are made to the system, they are approved and supported by documentation. ■ There is a person responsible for investigating security incidents that are reported. The incident, follow-up, and disposition are documented.	Concern for the integrity of data and that transactions are not altered or deleted.	Policies and procedures. Change logs. Security incident logs.

[25] The actual application may not change but the operating systems will change periodically. There may also be upgrades to the package applications (payroll, tax rates paid by the government, etc.).

Control	**Demonstrates**	**Entity Documentation**
Entity backs up, retains and stores important financial data and programs. Backups are stored in secure locations.	Commitment to accurate financial reporting.	Policy and procedures.
Management reviews the general computer controls of third-party vendors.	Commitment to accurate financial reporting.	SSAE 18 (formerly SSAE 16/SAS 70) reports or other means of reviewing the general computer controls where an SSAE 18 report is not available. A Type 2 report is preferable as it includes tests of the operating effectiveness of controls.
There are restrictions to access of computer equipment, telephone, network, and power supply.	Commitment to accurate financial reporting.	Policies and procedures.
There are **input** controls over transactions to ensure that they are authorized and processed completely and accurately. ■ Procedures to review data that is manually entered into the application including identifying, correcting, and reprocessing rejected data. ■ The system has input edits to check for invalid field lengths, invalid characters, missing or incorrect data and incorrect dates. ■ Input data is reconciled to source documents by control totals, batching techniques or other type of log. ■ Authorized person approves input documents.	Commitment to accurate financial reporting.	Policies and procedures, including review of packaged system documentation, logs, reports, and reconciliations.
There are **output** controls that assess whether input errors are reported and corrections made so that data will not be incomplete or inaccurate. ■ Output data is balanced or reconciled to source document. ■ Methods for balancing and correcting errors in output are explained. ■ Output is reviewed for general acceptability and completeness.	Commitment to accurate financial reporting.	Policies and procedures, logs, reports and reconciliations.

Control	Demonstrates	Entity Documentation
■ Error reports and logs contain information about any problems or errors, the date identified and corrective action taken. They are reviewed on a timely basis.		
Management uses a formal process for selecting new package.	Commitment to accurate financial reporting.	Criteria, documentation of decisions.

SPREADSHEET USAGE AND CONTROLS

Most entities use spreadsheets in a variety of ways, such as:

- In operations for tracking and monitoring workflow to support operational processes
- For analytical review on the part of management
- For financial reporting purposes

Unlike financial reporting systems, anecdotal evidence would suggest that there are few, if any, internal controls related to the use of spreadsheets to generate information that becomes part of the financial reporting process. In a past issue of Computer World, it was noted that audits of 54 spreadsheets found that 49 or 91% had errors.

The larger and more complex the spreadsheet, the more likely it is to have errors (inherent risk). Examples of complex spreadsheets are used in financial modeling, to construct valuations, and to support other complex calculations, are more likely to have errors. Errors usually take the form of input errors, logic errors, and errors that come from inappropriately defining cell ranges or spreadsheet links.

PricewaterhouseCoopers[26] (PwC) mentions nine potential risks and issues with spreadsheets to consider:

- Complexity of the spreadsheet and calculations
- Purpose and use of spreadsheet
- Number of users of the spreadsheet
- Type of potential input, logic and interface errors
- Size of the spreadsheet
- Degree of understanding and documentation of the spreadsheet requirements by the developer
- Uses of the output

[26] The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley Act, PricewaterhouseCoopers, July 2004.

- Frequency and extent of changes and modifications to the spreadsheet
- Development, training and testing of the spreadsheet before use

Management should inventory its spreadsheets that provide information incorporated into the financial statements or disclosures. Once the inventory is complete, each spreadsheet should be evaluated for its complexity. Management needs to implement controls over spreadsheets that generate significant operating information and when the resulting calculations are material to the financial statements. Material misstatement risk increases when spreadsheets are:

- Significant to the financial statements
- Complex
- Used by a number of client personnel
- Prepared by less qualified personnel

Following is a format that an entity could use to document controls over the preparation and review of significant spreadsheets.

Control	**To be Performed by**	**Time Frame**
Identify areas where spreadsheets are used to calculate amounts that will become part of the financial statement account balances, classes of transactions or disclosures.		Yearly
For each significant spreadsheet, a person independent of the preparer checks: Mathematical accuracy Assumptions and logic in the spreadsheet		When amounts are recorded in the financial statements. This may be monthly, quarterly or annually.
Alterations to a spreadsheet must be approved by an appropriate level of management/owner.		When alterations are made.
Output of spreadsheet is tested for reasonableness.		When amounts are recorded in the financial statements.

Spreadsheets that play an important role in the financial reporting process should have the following controls (and documentation):

- In writing, explaining the spreadsheet's purpose, how the spreadsheet works, linkages with accounting applications modules, and listing key spreadsheet specificationsChange management and version control process so only the latest, tested version is used
- Access controls

- Development controls
- Protected formula cells
- Testing of the spreadsheet calculations, relationships, and linkages before using its output in financial reporting

EXAMPLE

Reviewing Cost Overruns by Competent Personnel

The CFO of Home Builders of Raleigh, Frances Treat, reviews the process for controlling cost overruns. She determines that George Laurent, project manager, is indispensable. He understands client needs and project requirements, and effectively analyzes the effect of alternatives on project costs, schedules, and lifetime revenues.

Mr. Laurent reviews actual costs and indirect cost allocation. He ensures that change orders and potential overruns do not exceed authorized funding. He investigates variances and estimated costs for reasonableness, taking current stage of construction into account.

Ms. Treat understands that the spreadsheets Mr. Laurent uses could have errors so the controller tests the spreadsheets before any information is used in analysis or included in the financial reporting system.

Control Objectives for Information and Related Technology (COBIT)

The Information Systems Audit and Control Association developed COBIT, which is a framework for information technology and management. In this light, COBIT is similar to COSO because it places controls within the contest of specific objectives and the risks organizations incur towards achieving these objectives. COBIT takes a broader view and does not primarily focus on financial reporting.

COBIT is a supportive tool for managers and ties together information technology, business risks, and control requirements. Overall, COBIT enhances quality, control, reliability and integrity of information systems.

The COBIT business orientation links business goals with the business' information technology infrastructure by measuring goal achievement while identifying associated business responsibilities of information technology processes. COBIT has a process-based model subdivided into four specific domains:

- Planning & Organization
- Delivering and Support
- Acquiring & Implementation
- Monitoring & Evaluating

The various COBIT components include:

- **Framework** – organizes information technology governance and brings in the best practices in information technology processes and domains (above), while linking business requirements.

- **Process Descriptions** – serve as a reference model and is a common language for organization employees. Process descriptions include planning, building, running, and monitoring information technology processes.

- **Control Objectives** – provides requirements for effective information technology business control.

- **Maturity Models** – accesses process maturity, capability, and gaps.

- **Management Guidelines** – supports assigning responsibilities, measuring performances, agreeing on common objectives, and developing better interrelationships with other processes.

COBIT's guiding principles are:

- Meeting stakeholders' needs

- Covering the whole enterprise from end to end

- Application of a single integrated framework

- Ensuring a holistic approach to business decision making

- Separating governance from management

Principle 12. The Organization Deploys Control Activities Through Policies That Establish What Is Expected and in Procedures That Put Policies into Action. There Are Several Points of Focus

COSO principle 12 assesses important controls over daily accounting transactions, accrual estimates, and the financial close process. Principle 12 has six focus points about control policies and procedures.

1. Management Establishes Policies and Procedures to Support Deployment of Management's Directives

   A policy is management's statement of what should be done and may be written or unwritten. A procedure consists of actions that implement a policy.

   Most organizations have detailed descriptions of accounting policies and procedures for daily transactions, making estimates, periodic adjusting entries, account management, and for the accounting close. These organizations also have separate accounting and financial control documentation.

   Unwritten policies may be effective and lower-cost in small entities if existing policies are long-standing and well-understood. The risk is that unwritten policies are easier to circumvent, reduce accountability, and become more costly with high employee turnover. One in-between small-company approach could be documenting only unique accounting situations.

COSO does not prescribe specific documentation formats. Best practices are flow charts with explanatory narratives for each accounting process with controls incorporated and highlighted.

2. Management Establishes Responsibility and Accountability for Executing Policies and Procedures

   A policy must establish clear responsibility and accountability, with clarity on the responsibilities of personnel performing the control. Policies must be deployed thoughtfully and conscientiously, and the related procedures timely performed diligently and consistently by competent personnel.

   Management needs to develop lines of responsibility and authority levels which are communicated through formal documented policies. This way, undefined situations and potential exceptions have an oversight and approval channel.

3. Management Specifies that Controls Must be Performed in a Timely Manner

   Management designs procedures that specify when a control and any corrective actions should be performed.

   Management needs to implement signals about timing deviations, such as progress tracking and exception reports. Ideally, these are automated system signals that do not require employee intervention to produce. Other deviations are actual versus budget variances for operating metrics, department spending, division performance, or total organization performance.

4. Management Ensures that Corrective Action is Taken in Response to Issues Identified

   In performing a control, matters identified for follow-up should be investigated and corrective action taken if needed.

5. Management Ensures that Controls are Performed by Competent Personnel

   A well-designed control cannot be performed unless the entity uses competent personnel with sufficient authority.

6. Management Reassesses Policies and Procedures

   Management periodically reassesses policies and procedures and related controls for continued relevance and effectiveness. This is especially critical with today's rapidly-evolving business environment and rapidly-changing technology. The risk assessment process often identifies controls most-likely to be impacted by business or technology changes.

EXAMPLE

Controlling Significant Accounting Estimates

The CFO at Flower Herbal Oils prepares monthly valuation estimates for trade receivables. Factors considered include:

- Historical uncollectible percentages
- Historical collections and write-offs for specific customers
- Judgment on customers' ability to pay and intent

Judgments are inherently subjective and susceptible to error, so there are a mix of control activities intended to mitigate this, including:

- Treasurer reviews customers' Dun & Bradstreet information
- Automated preventive controls within ERP system
- Specific customer adjustments must be supported by reasons and analyses
- Assistant controller approves specific adjustments based on review of above reasons and analyses
- Controller assesses reasonableness of final estimate, considering rationale for historic percentage, rationale for material adjustments, consistency with knowledge of industry, business and customer trends and events

EXAMPLE

Establishing Responsibilities for Reviewing Financial Statements

Moonglow Lighting Corp. (MLC) installs lighting fixtures in Aiken, South Carolina. The company has policies dividing responsibility for review of financial statement information:

Nora Kline, the corporate controller, is responsible for reviewing the initial draft of the financial statements and financial reporting package:

- Review reconciliations and analyses to ensure preparation according to the corporate financial reporting handbook
- Review the financial reporting checklist to ensure preparation according to GAAP
- Review internal financial reports that discuss any material or unusual items that require judgment in presentation or disclosure
- Review comments on initial draft
- Submit final draft to CFO and disclosure compliance committee

Walter Burke, the CFO, is responsible for reviewing the final draft and summary of matters requiring resolution:

- Discuss the results of her review with Ms. Kline
- Read the final draft to identify any potential material misstatements or omissions
- Evaluate proposed resolutions of specific items, and decide which to pass on to the disclosure compliance committee
- Approve the financial statements after review by the disclosure compliance committee

- Present the financial statements and related items to the CEO and the audit committee for review and approve

The disclosure compliance committee is composed of the COO, CFO, and seven other senior managers including the controller. The committee reviews the final draft:

- Discuss their reviews with Ms. Kline and Mr. Burke
- Review all information to be published, including draft wording
- Concur with proposed resolutions of specific matters or send back to functional management for more research and recommendation
- Oversee disclosure procedures and coordinate disclosure to external parties
- Inform CEO and CFO of any issues identified

NOTES

Unit 8

Information and Communication

LEARNING OBJECTIVES

After completing this unit, participants will be able to:

☐ Explain the FASB's Concept Statement on decision usefulness

☐ Explain COSO information and communication principles

☐ Recognize bias

INFORMATION AND COMMUNICATION

The COSO framework lists the following three principles related to the information and communication components of internal control. Technology advances have created two changes with information and communication. First, organizations can produce almost unlimited information. This means they can use data to increase operational and financial transparency or make them more opaque.

Secondly, organizations can reach stakeholders at almost zero communications costs, which means organizations increasingly can easily bury stakeholders (management, the board of directors, auditors) in data. Too much detail can overwhelm the recipient as well as obscure relevant situations. Data are different from information because data are unanalyzed figures. Information is analyzed date with insights, meaning, and conclusions.

Decision Usefulness and Financial Reporting

The objective of financial reporting is to provide useful measures and disclosures about an entity's financial performance and financial condition. Users of financial reports employ financial analytical techniques to assess management's performance in creating value historically and to forecast future value. From this financial analysis, users of financial reports make operating, investing, and financing decisions.

The Financial Accounting Standards Board (FASB) formally addressed financial reporting as early as 1978 when it published the first of a series of eight concepts statements (CON)s. CONs main purpose is to establish the foundation for the FASB's financial accounting and reporting guidance development. CONs are not codified, and, thus, are not authoritative GAAP.

A secondary purpose is CONs also enable financial statement users to understand the content and limitations of accounting and financial information they use in performing financial analysis. Together with information from other sources, CONs serve financial information users by facilitating efficient functioning of capital and other markets which promotes efficient allocation of scarce resources based on users' financial analysis.

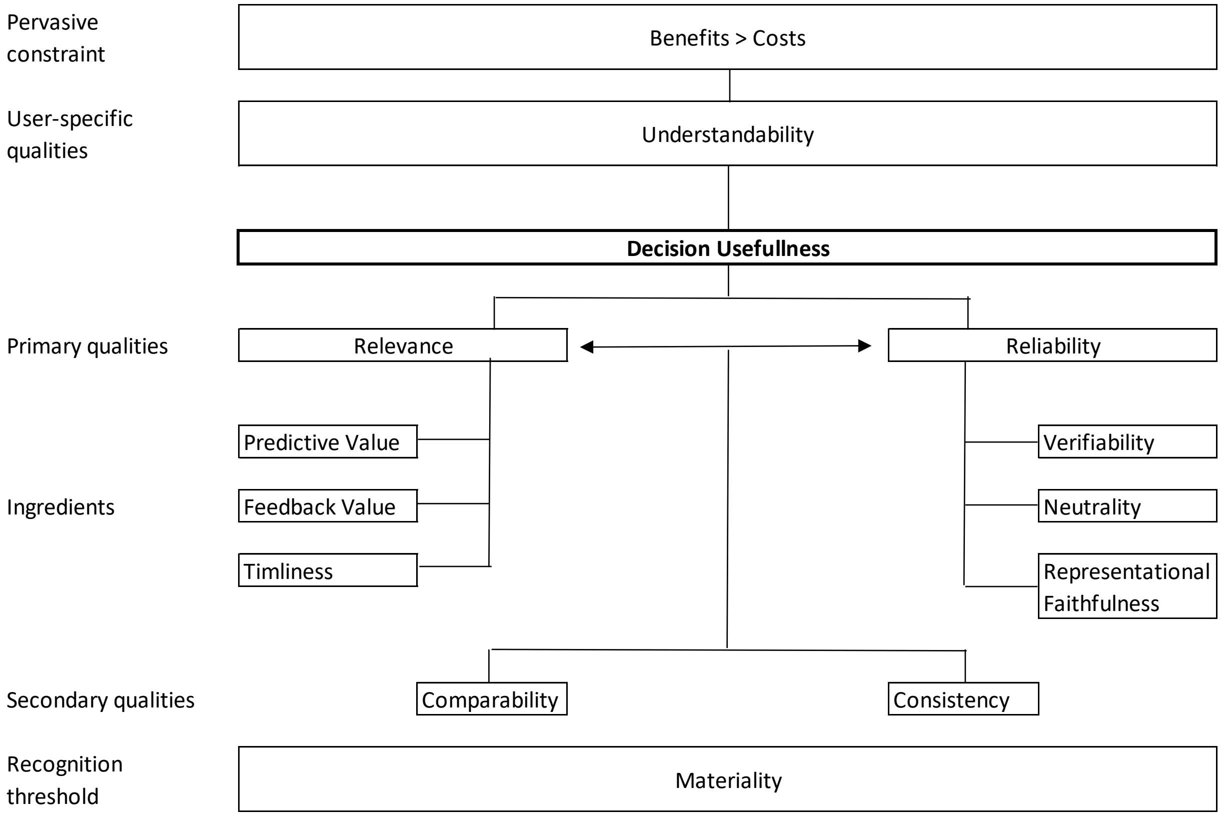
Underlying this section is the following Statement of Financial Accounting Concepts (SFAC)s as they apply to users of financial reporting. SFAC and CON are interchangeable terminology.

- SFAC No. 8, Conceptual Framework for Financial Reporting, issued in 2010
  - Superseded SFAC No. 1, Objectives of Financial Reporting by Business Enterprises, issued in 1978
  - Superseded SFAC No. 2, Qualitative Characteristics of Accounting Information, issued in 1980
- SFAC No. 6, Elements of Financial Statements, issued in 1985
  - Superseded SFAC No. 3, Elements of Financial Statements of Business Enterprises, issued in 1980. It expanded the scope to encompass not-for-profit organizations.

Financial statements communicate historical data, which is most useful for current-state compliance purposes, such as filing with, providers of debt and equity financing, tax authorities, and other regulatory agencies. It is also useful for assessing management performance and compensation awards. While financial reporting tells us "where we've been," users must apply financial analytical techniques to tell us "where we're going." As a result, five themes underlie financial statement analysis:

- The types and uses of financial analysis depends on the user and the decision the user is making.
- In most cases, financial statement analysis involves using historical data to assess past performance and to make judgments about future potential performance. CON No. 2 (superseded by CON 8), shows a decision usefulness diagram and specifies qualitative ingredients that financial and accounting information should possess to be useful for making decisions.

A HIERARCHY OF ACCOUNTING QUALITIES
for users (decision makers) of financial information



Decision usefulness is based on primary qualities of relevance and reliability as well as secondary qualities of comparability and consistency. Financial statement users must assess both these qualities. Following are decision usefulness quality definitions.

- Relevance is the capacity of information to make a difference in a decision by helping users to form predictions about the outcomes of past, present and future events or to confirm or correct prior expectations.
    - Predictive value is the quality of information that helps users to increase the likelihood of correctly forecasting the outcome of past or present events.
    - Feedback value is the quality of information that enables users to confirm or correct prior expectations.
    - Timeliness is having information available to a decision maker before it loses its capacity to influence decisions.
- Reliability is the quality of information that assures that information is reasonable free from error and bias and faithfully represents what it purports to represent.

  - Verifiability is the ability through consensus among measurers to ensure that information represents what it purports to represent or that the chosen method of measurement has been used without error or bias.

  - Neutrality is the absence in reported information of bias intended to attain a predetermined result or to induce a particular mode of behavior.

  - Representational faithfulness is correspondence or agreement between a measure or description and the phenomenon that it purports to represents. This is also referred to as validity.

- Comparability is the quality of information that enables users to identify similarities in and differences between two sets of economic phenomena.

- Consistency is conformity from period to period with unchanging policies and procedures.

CON No. 2 (superseded by CON 8) also states that financial reporting should be practical and shows a pervasive constraint that the financial reporting costs should not exceed their benefits. As an example, materiality is shown as a recognition threshold; meaning that if the transaction monetary value is too small to impact a decision, then the entity should account for the transaction in the most efficient manner.

- Financial analysis should incorporate broad sources of financial and non-financial information about an entity. This includes entity-specific financial statements including note disclosures. It also includes non-entity-specific industry, economic, and political environmental information. This information can be critical to understanding an entity's financial status, business and financial performance, and future prospects.

- GAAP (accrual) based analysis can be prone to distortion due to the uncertainty of estimates and judgments made by management, or changes in accounting standards.

- As a result of #4, cash-flow-based analysis may be better suited for evaluating a reporting entity's earnings quality and financial flexibility in dealing with changing business, competitive, and economic conditions or with pursuing new opportunities. While earnings can be manipulated through **biased** estimates or alternative GAAP applications, cash flow measurements are more difficult for management manipulation.

Bias is a behavioral trait that impacts human decision making. Unintentional bias is rarely obvious to those making decisions and requires conscious introspection. Thus, good managers may make unethical decisions without knowing it.

Professional skepticism in accounting is attitudes of a questioning mind, alertness to conditions that could indicate possible misstatement due to error or fraud. It plays an important role is assessing management and employee assertions as well as assessing financial, accounting, and audit evidence.

Some bias examples that may impact financial reporting are:

- **Conformity bias** – the tendency to behave similarly to the people around oneself regardless of one's personal beliefs. There may also be pressure that causes a person to subordinate their own thinking or beliefs. Culturally, conformity bias would be reflected as "go along to get along."

  A similar concept is groupthink, which is when a group decision becomes influenced by the strong personality of the highest-ranking person present. This generally occurs within team dynamics.

  As an example, when a team meets to discuss whether to recognize a liability, conformity bias can cause individuals to agree to the opinion of the majority. The problem is the majority is not always right. Another example is the book by Bethany McLean and Peter Elkind, E*nron: The Smartest Guys in the Room*, about one of the largest business scandals in American history.

  One method to reduce conformity bias would be to ask each team member to provide their individual opinions separately. Subsequently bring the team together and review these impartial opinions.

- **Confirmation bias** – the tendency to look only for and to place greater value on information that supports one's personal beliefs or position and disregard information that does not. In accounting, this may manifest itself by operating on automatic pilot by performing one's job the way we always have, or by following the same decision path.

  An example would be deciding whether to disclose summary financial statements of a material equity-method investment. If the investment were immaterial in previous periods, that may not be true this period. Potential reasons could be the reporting entity may have become smaller due to spinoffs or deteriorating operations, or the equity-method investment could have become larger due to acquisitions or strong operating performance. Either situation could result in the equity-method investment becoming material and requiring greater disclosures.

  One method to reduce confirmation bias is to develop a standardized methodology to decision making or by following checklists.

- **Overconfidence bias** – the tendency for someone to overestimate their capabilities or subject knowledge. In addition, overconfidence bias can exacerbate the impact of other biases listed here because one may ignore their vulnerability to bias and error.

  One method to reduce overconfidence bias is to have peers independently review their work. Another way would be to create one's personal board of directors, especially for a successful person to help keep them grounded.

- **Availability bias** – the tendency to utilize only easily-available information. This may be data that one already possesses or that is easy to obtain. This may result in improperly evaluating financial information or not performing all of the proscribed steps in the evaluation or decision-making process. Another result may be taking process shortcuts.

Decision makers tend to be more influenced by what they remember, which can be caused by high exposure frequency. Media coverage on television, radio, and print as well as digital media on the Internet makes a big difference. Thus, people may place greater importance to events the ease and sequence that they can retrieve from memory.

One may believe that a recollection is factually correct while discounting events that are outside of immediate memory. For example, if someone is an automobile accident, they may become ores likely to assess the probability of getting into another car accident at a much higher level than reality.

- **Framing bias** – the tendency to make decisions from option presented under a positive or negative perspective. Gains and losses are a frequent framing situation. A loss is perceived as more significant, and thus more worthy of avoiding, than an equivalent gain. In another example, 80%-lean ground beef is viewed better than 20%-fat ground beef. Both choices, however, are identical.

  One method to reduce framing bias is through employee ethical and risk assessing training.

Users of financial statement information are presumed to have a reasonable understanding of business and economic principles. To effectively analyze financial statement information, users must gain knowledge concerning the company's industry, past experience, competitors, and financial trends. Financial statement users must also become knowledgeable about changing business, economic, and regulatory conditions or operational changes affecting the entity.

External (owners and creditors) and internal (management) financial statement users generally make three types of decisions from their financial analysis.

1. Operating
   - Effective asset utilization
   - Business performance
   - Profitability
   - Operating leverage
   - Liquidity
2. Investing
   - Capital budgeting for committing funds to working capital, new plant and equipment, and major strategic initiatives
   - Disinvestment by disposing of significant assets or withdrawing from markets
3. Financing

- Capital structure
- Returns on capital
- Types of equity and debt
- Risk tolerance
- Dividend policy

Principle 13. The Organization Obtains or Generates and Uses Relevant, Quality Information to Support the Functioning of Internal Control

This guidance is to identify controls over accounting and general information processes that ensure providing complete, accurate, timely, and cost-effective information to employees that need that information to achieve their objectives. Timing is critical to provide information while it is still useful for controlling the organization's operating activities and financial reporting.

There are five focus points for principle 13:

1. Management Identifies Information Requirements

   Obtaining relevant information requires management to identify and define information requirements at the relevant level and with requisite specificity. This is an ongoing and iterative process.

2. Management Captures Internal and External Sources of Data

   The information system captures relevant financial and non-financial data which is used to prepare financial and operating reports that impact operations, finance & accounting, and regulatory reporting needs. The data are both financial and non-financial, and both impact financial reporting and disclosures as well as operating performance. Organizations need processes to capture and analyze these data.

   Support for management judgment of accrual estimates often rely on non-financial information. An example of external non-financial data impacting financial reporting would be the allowance for doubtful accounts. Management would need data to assess economic conditions for the overall economy, for specific industries, and for individual companies.

   Another example supports management assessing concentration risk which has important accounting disclosure, strategic, and operating impacts. Examples of internal non-financial data impacting operating performance would be on-time customer deliveries, scrap rates, or customer complaints. External data impacting operating performance could be market share.

   The information system captures data from a variety of sources and in a variety of forms. Examples are:

- Internal data:
  - Organizational changes
  - On-time and quality production experience
  - Actions in response to energy consumption metrics
  - Hours incurred on time-based projects
  - Units shipped in a month
  - Factors impacting customer attrition
  - Complaint on manager’s behavior
- Internal data sources:
  - Email
  - Inspections of production processing
  - Committee minutes, notes
  - Personnel time reports
  - Manufacturing systems reports
  - Customer surveys
  - Whistleblower hotline
- External data:
  - Products drop-shipped
  - Competitor information
  - Market and industry metrics
  - New or expanded requirements
  - Opinions about the entity
  - Customer preferences
  - Claim of misuse of funds, bribery
- External data sources:
  - Data from outsourced providers

    - Industry research reports
    - Peer company earnings reports
    - Regulatory bodies
    - Social media, blogs
    - Trade shows
    - Whistleblower hotline

Risks can arise in several ways that are internal or external to the entity. For example:

- Management Ensures that the Systems Processes Relevant Data into Information

  Information systems capture and process large volumes of data from internal and external sources into meaningful, actionable information to meet defined information requirements.

  The AICPA issued AU-C No 315, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement (PCAOB AS 2110). Although issued for auditors, AU-C 315 provides important information for organizations. The AU guidance for describes necessary elements of an information system for financial reporting:

  - Identify and record all valid transactions
  - On a timely basis, describe the transactions in sufficient detail for proper transaction classification for financial reporting
  - Measure transaction monetary value properly for recording in the financial statements
  - Determine the time period that transactions occurred for recoding in the proper accounting period
  - Present the transactions and related disclosures properly in the financial statements

- Management Ensures that Systems Maintain Quality throughout Processing

  Maintaining quality of information is necessary to an effective internal control system. The quality of information depends on whether it is:

  - Accessible – easy to obtain by those who need it
  - Correct – accurate and complete
  - Current – most recent

- Protected – access to sensitive data restricted to authorized personnel
- Retained – properly and securely stored
- Sufficient – enough information, right level of detail, extraneous eliminated
- Timely – available when needed
- Valid – represents events that actually occurred
- Verifiable – supported by evidence from the source

■ Management Considers Costs and Benefits of Internal Controls

The nature, quantity, and precision of information communicated are commensurate with and support the achievement of objectives.

EXAMPLE

Conducting Quarterly Interviews of Operations and Other Management

Fishy Charlie's is a supplier of fresh seafood to restaurants and other commercial accounts. The controller, Arnold Zimmer, is responsible for a monthly evaluation of inventory reserves. In the past, there were problems with this evaluation because of significant fluctuations in usage trends, customer product preferences, purchase commitments and other unanticipated changes. As a result, Arnold now uses reports from the company's information system to identify unanticipated or unusual trends or changes in inventory inflows, outflows and balances. He then meets monthly with several department heads to collect additional information affecting inventory. Based on these meetings, Arnold reviews inventory reserve policies including how they were calculated in the past, and prepares updated reserve requirements. He then submits his report to the CFO for review and approval.

EXAMPLE

Obtaining Operating Information for Financial Reporting

Hammond Texas Petroleum is an independent oil and gas exploration and production company with operations in Texas, North Dakota and Manitoba. Because petroleum-related operations have the potential to cause significant environmental damage, the company is subject to stringent Federal, Canadian, state and provincial regulations, all of which carry heavy financial and operational penalties for violations. In addition, surface landowners may be entitled to damages if the company contaminates their land. Adrienne Chateaux, the controller, receives monthly operational and compliance reports from the COO. She also reviews internal audit reports as they relate to environmental compliance. She uses this information to assess reserves or disclosures that may be required for environmental fines or damages, and meets with the CFO quarterly to decide whether any changes are needed in financial statement disclosures or accounting estimates.

Principle 14. The Organization Internally Communicates Information, Including Objectives and Responsibilities for Internal Control, Necessary to Support the Functioning of Internal Control

Organizational communications are both formal and informal. Formal communication includes policies & procedures manuals, mission statements, process documentation, memos, e-mail, blogs, and posters placed in areas where employees congregate such as lunch rooms. Informal communication includes customer communications (which can become formal if documented into a CRM system), meetings, and presentations.

Monitoring controls are highly dependent on effective communications and include management reviewing operating and financial results, board reporting and governance, and regulatory compliance. For many control activities to function properly, an organizations' information and communication systems must be integrated with its control activities. For example, early timing of detecting variances or producing exception reports that impact achieving operating goals or preventing fraud.

Good communications with employees, management, and overseers that perform control functions impacts control effectiveness. Examples are:

- Overall internal control system – objectives
- Specific control activities – specific performance requirements and employee duties
- Interrelationships and alignment – how specific control activities impact other control activities as well as within a control activity how specific employee duties impact other employee duties
- How to communicate – monitoring of control performance results, especially unfavorable variances or control weaknesses
- What actions to take – when receiving notice of performance results, especially unfavorable variances or control weaknesses. This includes policies & procedures and change management processes.

Employee behavior – what is acceptable and unacceptable

There are four focus points for principle 14:

1. Management Communicates Internal Control Information
    - Communication of information conveyed across the entity include:
        - Policies and procedures that support personnel in performing their internal control responsibilities
        - Specified objectives
        - Importance, relevance, and benefits of effective internal control

    - Roles and responsibilities of management and other personnel in performing controls
    - Expectations of the organization to communicate within the organization any significant internal control matters including weakness, deterioration, or non-adherence

2. Management Communicates with the Board of Directors
    - Communication between management and the board provides the board with information needed to exercise its oversight responsibility for internal control. Frequency and detail must be sufficient to enable the board to timely respond to indications of ineffective internal control.

3. Management Provides Separate Communication Lines
    - For information to flow up, down, and across the organization, there must be open channels of communication and a clear willingness to report and listen. In some circumstances, separate lines of communication are needed, such as whistleblower and ethics hotlines and anonymous or confidential reporting via information systems.

4. Management Selects Relevant Method of Communication
    - Clarity of information and effectiveness with which it is communicated are important to ensure messages are received as intended. Communication can take such forms as:
        - Dashboards
        - E-mail
        - Live or on-line training
        - Memos
        - One-on-one discussions
        - Performance evaluations
        - Policies and procedures
        - Presentations
        - Social media postings
        - Text messages
        - Webcast and other video
        - Website or collaboration site postings

- Management considers that when choosing a communication medium, for messages that are transmitted orally, tone of voice and nonverbal cues are very important. In addition, cultural, ethnic, and generational differences can affect how messages are received.

- Management is aware that communications relevant to internal control may require long-term retention or employee review and acknowledgement (e.g., code of conduct, corporate security).

- Management is aware that time-sensitive communications may be more cost-effectively delivered through informal media such as email, text messaging or social media.

- Management is aware that communications solely through formal means (e.g., official memos) may not reach their intended audience and may not receive return communications from those more comfortable with email, text messages, social postings, etc.

EXAMPLE

Using Communications Programs to Reinforce Internal Control

Casas Por Todos is an international charity that operates in four countries in South America constructing houses for those who could not otherwise afford them. The CEO, Jim Carrera, frequently travels to Casas Por Todos sites around the world to keep in contact with the charity's local staff, but between visits uses broadcast emails to keep relevant staff updated on accounting, finance, and other external financial reporting related issues. He also uses local visits to reinforce expectations that staff follow internal control policies and practice strict adherence to laws and regulations. The CFO, Tammy Vining, also travels and uses emails to discuss topics on business objectives and goals, and progress toward them. On her local visits, she meets with staff to find out how well they understand the charity's key business and financial goals and to also reinforce understanding and appreciation of internal control policies.

EXAMPLE

Preparing Financial and Internal Control Reporting Package for Discussion with the Board

Beyond Logistics Corp. is a private space launch firm and has a contract with NASA to deliver cargoes to the International Space Station. Senior management at Beyond Logistics has prepared a financial and internal control report package for the upcoming board of directors meeting. The package includes quantitative and qualitative internal control as well as financial reporting information, highlighting trends and other matters requiring the board's attention. It includes discussion of the dollar impact of significant adjustments, estimated impact of deficiencies, new regulatory requirements, changes in accounting policies, and significant changes in the company's financial statements and disclosures. Management delivers the package to board members early enough to allow members adequate time to review it before the meet.

Principle 15. The Organization Communicates with External Parties Regarding Matters Affecting the Functioning of Internal Control

Public companies have well-defined clear guidance for financial reporting and disclosures. For non-public companies, debt agreements and shareholder rights agreements establish financial reporting and disclosure requirements. In addition, there are formal and informal communication channels for supply chain communications, community relations, and government and regulatory reporting.

Organizations need established policies and procedures as well as controls for external communications. This includes approval processes and what managers are authorized to communicate externally. For example, what criteria determine which events require external communication, appropriate timing, and which external communications need legal or board review. Another example is that public companies can violate SEC regulations (Regulation FD) by communicating material information to select shareholders or stakeholders but not others.

With the accelerating advances in social media, such as blogs and Twitter, external communications policies, procedures, and controls are much more important. Organizations need clearly communicated policies for external communication of organization matters.

There are five focus points for principle 15:

1. Management Ensures that the Level of Communication to External Parties is Appropriate

   – Management develops and implements controls that facilitate external communication. Outbound communication should be viewed distinctly from external reporting. Communication to external parties allows them to readily understand events, activities, or other circumstances that may affect how they interact with the entity.

2. Management Enables Inbound Communications

   – Communications from external parties may provide important information on the functioning of the entity's internal control system. These can include:

     - Outsourced independent internal control assessment
     - Auditor's internal control assessment
     - Customer feedback, especially complaints
     - New or changed laws, regulations, etc.
     - Regulatory compliance review results
     - Vendor questions, especially payment complaints
     - Social media postings, especially on entity-sponsored site

3. Management Enables Communications from External Parties to the Board of Directors

   – Relevant information resulting from assessments conducted by external parties is communicated to the board.

4. Management Provides Separate Communication Lines

   – Separate communication channels, such as whistleblower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.

5. Management Selects Relevant Method of Communication

   – The medium by which management communicates externally affects its ability to obtain information needed as well as to ensure that key messages about the organization are received and understood. It should take into account the audience, nature of the communication, timeliness, and any legal or regulatory requirements.

   – Following are examples of approaches that small to mid-size entities can use to implement controls related to communication, along with documentation that they should consider to evidence that control's implementation. Adequate documentation makes it easier for the auditor to perform risk assessment procedures. When the entity does not provide adequate documentary evidence, the auditor is challenged to accomplish the observation and inspection.

   – Note that the examples listed below are options for the entity. Not every entity will implement every control. The auditor's task is to determine that the communications process is appropriately designed as a whole, not that every possible control is implemented.

EXAMPLE

Establishing Periodic Communications with Contractors and Outsourced Service Providers

Midgard Mining (Midgard) manufactures mining and earth-moving machinery. More than half of Midgard's manufacturing is done offshore by third parties, located primarily in Asia and South America. Midgard contractually bears the risk of loss or damage of inventory while in the third party's possession. This gives Midgard a much better price from its contract manufacturers, but leaves it with significant liability for occurrences beyond its physical control. Midgard controls this risk using an extensive and rigorous system of policies and procedures covering purchasing, manufacture, and preparation for shipment. This system is reinforced by specific contract clauses requiring policy adherence and the right to audit. Midgard maintains communication with its contract manufacturers using a dedicated website, a link on the website to Midgard's policies and procedures which the contractors are required to acknowledge and accept, a variety of periodic reports from the contractors, periodic on-site contractor audits including detailed physical inventories, and annual reviews of contractor controls to support their reports.

Midgard also uses a service organization to handle its 401K plan processing. The CFO obtains a System and Organization Controls Report (SOC) each year. The CFO evaluates the type of the report to ensure it is a Type 2 SOC 1 report. He also evaluates the opinion to determine if it was unmodified, that any findings were not significant and that the user controls suggested are in place at Midgard and operating effectively.

EXAMPLE APPROACHES THAT SMALL TO MID-SIZE ENTITIES CAN USE

Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control over financial reporting.

- Relevant operating information is used to develop accounting and financial information and serves as a basis for reliable financial reporting. Operating information is used as the basis for accounting estimates.
- Accounting procedures are sufficiently formal that management can determine whether the control objective is met, documentation supporting the procedures is in place, and personnel routinely know the procedures that need to be performed.
- Data underlying financial statements are captured completely, accurately, and timely, in accordance with the entity's policies and procedures and in compliance with laws and regulations.

Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, to support the functioning of internal control over financial reporting.

- Financial personnel meet with line management to discuss operating results.
- Information is collected in time to permit effective monitoring. Established and agreed-upon deadlines exist for period end reporting, which include review by management.
- The current chart of accounts is adequate to maintain accountability and provide for the level of detail that is required for the entity to manage
- Management communicates information about the functioning of internal control over financial reporting on a timely basis with those charged with governance.
- Employees receive adequate information to complete their job responsibilities.
- Management has developed communication approaches that specify individual responsibilities in dealing with inappropriate behavior.
- Upstream communication is encouraged by management to improve performance and enhance internal control.
- All reported potential improprieties are reviewed, investigated, and resolved in a timely manner.

Principle 15: The entity internally communicates with external parties regarding matters affecting the functioning of internal control.

- Management communicates information about the functioning of internal control over financial reporting on a timely basis with those charged with governance.
- All reported potential improprieties are reviewed, investigated, and resolved in a timely manner.
- There is a process for tracking communications from customers, contributors, vendors, regulators, and other external parties.

Note that communication needs to be two-way on multiple levels:

- Between management and employees

  - Employees should feel free and welcome to discuss issues with management. Channels should be available above senior management in case employees do not feel comfortable; for example, with a board member.

- Between management and vendors

- Between management and customers

- Between management and the board of directors

NOTES

Unit 9

Monitoring Activities

LEARNING OBJECTIVES

After completing this unit, participants will be able to:

☐ Explain COSO monitoring principles

☐ Use this understanding of monitoring principles in applying controls

MONITORING

One of Murphy's Laws is that it is impossible to make anything foolproof because fools are so ingenious.

Monitoring is a very important component of internal control, especially in a small business. Monitoring consists of almost any process that is used to ensure that controls are operating as designed, and can be used to help streamline management's assessment and review process. Monitoring can point out indications or evidence of fraud or error. Poor monitoring controls can allow fraud or error to remain undetected.

One of the most effective parts of internal control is monitoring so that management can be sure that their internal controls are functioning as designed. COSO believes that some management teams may not fully appreciate the power of monitoring when considering the effectiveness of internal controls. In 2009, COSO published its *Guidance on Monitoring Internal Control Systems*. This guidance is not intended to replace the COSO framework but is designed to highlight and expand the basic principles in both documents. This publication can be purchased from the AICPA's CPA2BIZ website.

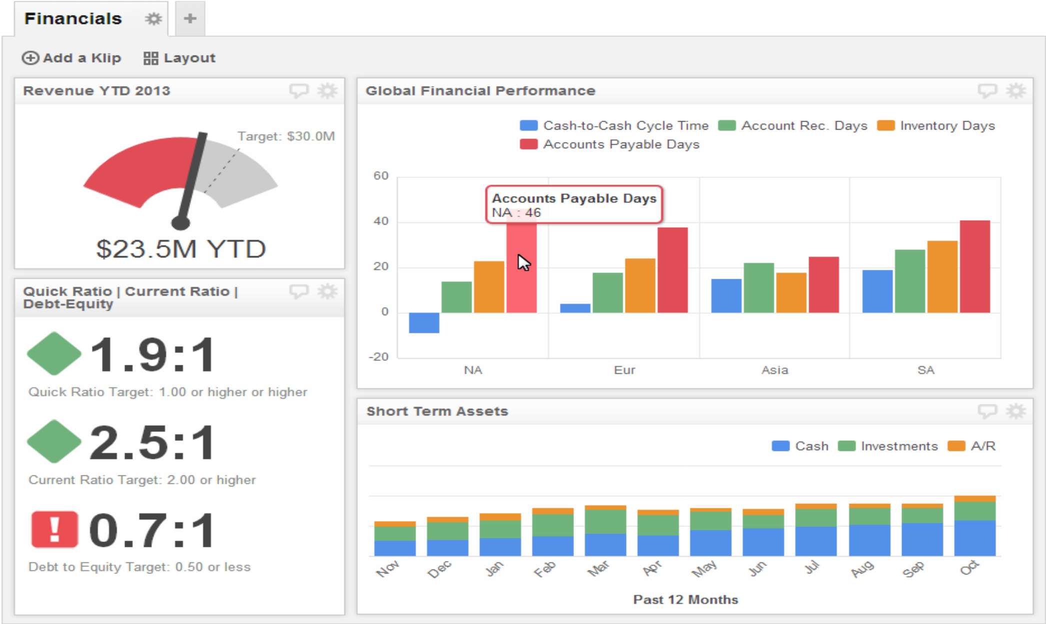
Monitoring activities can be ongoing or separate evaluations to determine if the controls continue to function over time. Another benefit of monitoring is that internal control deficiencies are identified more timely and can be communicated to management and in some cases, the board so they can take corrective action.

It is important that the entity establish a foundation for monitoring that includes the proper tone at the top. It is also important that the organization has a structure that contains monitoring roles. The people in those roles should be objective, have authority and, of course, the capability to perform the function. It is also important to establish a benchmark or baseline so that performance can be measured over time.

Every organization is responsible for monitoring control implementation and effectiveness as well as the quality of internal control performance over time. Management assesses control design and operation periodically. If management identifies any control deficiencies, it makes timely corrective improvements.

Best practice for organizations communicating monitoring activities is using a "dashboard" or "cockpit". An automobile dashboard or airplane cockpit display monitoring performance data with insight on good or bad in visual format. The visual all-encompassing approach communicates performance rapidly because management or those charged with governance can monitor several performance indicators on one page, instead of having to read and analyze multi-page reports. Updating the organization dashboard more frequently approaches real-time performance monitoring, much like automobile dashboards. [27]

A financial dashboard example is shown below:



The COSO framework lists two monitoring principles.

Principle 16. The Organization selects, Develops, and Performs Ongoing and/or Separate Evaluations to Ascertain Whether the Components of Internal Control Are Present and Functioning

There are seven focus points to principle 16:

1. Management Considers a Mix of Ongoing and Separate Evaluations

[27] https://www.klipfolio.com/resources/dashboard-examples/executive/financial-performance

- Management selects, develops, and performs a mix of monitoring activities, usually including both ongoing and separate evaluations, to ascertain whether each of the five components of internal control is present and functioning.

- Separate control evaluations are different from ongoing evaluations because "triggers" drive separate evaluations. A trigger would be previously-identified control deficiencies, business processes changes, or risk assessment changes.

2. Management Considers Rate of Change

   - Management considers the rate that an entity or its industry is expected to change. In a quickly changing industry, an entity may need more frequent separate evaluations and may reconsider its ongoing/separate mix.

3. Management Establishes Baseline Understanding of the System of Internal Controls

   - Understanding the design and current state of a system of internal control provides useful baseline information for establishing ongoing and separate evaluations. If an entity lacks a baseline understanding in higher risk areas, it may need a separate evaluation to establish the baseline for those areas.

   - Effective monitoring through performing data analytics and trend analysis require a reliable baseline from which to identify variances. Examples would be revenue and cost trends, financial ratios, or determining other financial relationships such as the inventory obsolescence reserve as a percent of total inventory.

   - For multi-location organizations, the baseline may become a best demonstrated practice used to compare each location's financial and operational performance.

4. Management Uses Knowledgeable Personnel for Monitoring Tasks

   - Since separate evaluations are conducted periodically by independent managers, employees, or external reviewers to provide feedback with greater objectivity, evaluators need to be knowledgeable about the entity's activities and how the monitoring activities function, and understand what is being evaluated.

   - Monitoring requires judgment; therefore, it is not a mechanical task that can be delegated to inexperienced or low-level employees. An apparently insignificant, low-value improper payment identified during control monitoring could, instead, be part of a much larger fraud.

   - There are a variety of approaches available to perform separate evaluations, including:

     - Internal audit evaluations

     - Other objective evaluations

     - Cross-operating unit or functional evaluations

        - Benchmarking/peer evaluations

        - Self-assessments

    - Separate evaluations can be performed by:

        - Those responsible for the controls (control self-assessments)

        - Internal audit

        - Consultants

5. Management Integrates Ongoing Evaluations with Business Processes

    - Ongoing evaluations are built into the business processes and adjust to changing conditions.

    - Management adjusts scope and frequency of separate evaluations depending on risk and makes objective evaluations to provide good feedback

EXAMPLE

Using Metrics to Monitor Payroll

Hollywood to Go LLC (H2G) provides turnkey film production and location support services for clients including movie and television producers, advertising agencies and in-house corporate video producers. More than 80% of H2G's employees work on-site at support locations. To ensure that payroll control activities are working, Hank Miller, the corporate payroll manager, reviews various payroll metrics, including: Employee count vs. expected and historical for year, month and quarter; current payroll vs. expected and historical for year, month and quarter; and current overtime in hours and dollars vs. expected and historical for year, month and quarter.

In his review, Mr. Miller looks for unusual fluctuations such as in employee count and overtime. This review is done in the context of the volume of support jobs and seasonal variation. When significant unexplained variations are found, he adjusts the process or control activities as appropriate.

EXAMPLE

Understanding Controls at an Outsourced Service Provider

Miami Ultimate Seawalls Corp. is a leading builder of residential and commercial seawalls in the south Florida region. The company has outsourced its payroll processing to PayBux, a reputable payroll processor, for many years.

The following process was put in place related to reviewing the quality of outsourced providers.

Management obtains and reviews periodic information from outsourced service providers to detect any changes in activities that impact the entity's system of internal control over external financial reporting. Information obtained may include:

- The outsourced service provider's applicable control objectives
- Details about which of the outsourced service provider's internal controls have been examined and included in any report

- The details and results from any independent audit testing performed
- Special considerations for the outsourced service provider that impacts the report

To determine what impact any identified changes may have on the entity's system of internal control over external financial reporting, the following may also be assessed:

- Whether management appropriately considered known changes in business processes and their impact on internal control, and whether they were communicated to the outsourced service provider, since such changes could impact the entity's control objectives and design
- Whether exceptions were noted that may trigger further review by senior management
- Whether management is satisfied with the independence and objectivity of the report

Based on management's review and findings, it may be necessary to reassess the separate evaluation activities over the outsourced service provider.

In 20X1, Hearst Brenner, the CFO, received the annual service auditor's report on PayBux's internal controls. He then compared the current with previous reports to detect changes in PayBux's controls that could impact his planning for payroll process monitoring. The new report showed some changes in PayBux's software and some negative test results in high risk areas. In response, Mr. Brenner asked his accounting team to reconcile PayBux's processing results to determine if additional separate evaluations may be necessary.

6. Management adjusts monitoring scope and frequency
7. Management objectively evaluates control design, implementation, and operational effectiveness

Principle 17. The Organization Evaluates and Communicates Internal Control deficiencies in a Timely Manner to Those Parties Responsible for taking Corrective Action, Including Senior Management and the Board of Directors, as Appropriate

COSO broadly defines 'deficiency' to mean any internal control system condition worthy of attention. COSO also defines 'major deficiency' to be made up of severe deficiencies. The SEC and AICPA audit standards use different terms of 'significant deficiency' and 'material weakness'.

Very important, and often misunderstood by operating management, is that distinguishing between control deficiency levels does not depend on the misstatement size or whether there was actually a misstatement at all. The determinant is whether it is 'reasonably possible' that a misstatement **could** occur.

Principle 17 contains three focus points.

1. Management and the Board Assess Results of Monitoring Procedures

   – Management and the board regularly assess internal control for deficiencies; information comes from a variety of sources, including:

        - Ongoing evaluations
        - Separate evaluations
        - Other internal control components
        - External parties such as customers, vendors, external auditors and regulators

2. Management Communicates Deficiencies in Internal Control

    - Communicating internal control deficiencies to the right parties to take corrective actions is critical for entities to achieve objectives. In some cases, external reporting of a deficiency may be required by laws, regulations or standards.

    - Identified internal control deficiencies need to be reported to the individuals who are in the best position to take action as well as to those charged with governance. This may include reporting not only to the person directly responsible for the performing the control but also to at least one level of management above the directly-responsible person.

3. Management Monitors Corrective Actions

    - After internal control deficiencies are evaluated and communicated to those parties responsible for taking corrective action, management tracks whether remediation efforts are timely conducted.

    - When deficiencies are not corrected on a timely basis, management revisits the selection and deployment of monitoring activities, until corrective actions have remediated the internal control deficiency.

Examples of ongoing monitoring include:

- Periodic evaluation and testing of controls by internal audit (if any)
- Analysis of, and appropriate follow-up on operating reports or metrics that might identify indications of a control failure
- Management and supervisory activities where controls are reviewed
- Comparisons of budget to actual, comparisons from current year/periods to prior year/periods
- Reconciliations of account detail to the general ledger as part of the ongoing processing
- Continuous monitoring programs built into information systems that includes a review of exception reports generated by the system
- Audit committee (if applicable) inquiries of internal and external auditors
- Quality assurance reviews of the internal audit department, if applicable

- Self-assessments by boards and management regarding the tone they set in the organization and the effectiveness of their oversight functions

Following are examples of approaches that small to mid-size entities can use to implement controls related to monitoring, along with documentation that they should consider to evidence that control's implementation. Note that the examples listed below are options for the entity. Not every entity will implement every control.

EXAMPLE

Establishing Reporting Protocols for Identified Deficiencies

Senior management at Safety Engineering Systems reviews control deficiencies found during monitoring activities and analyzes their effect on the company. These deficiencies are reported to management of the affected business unit. If needed, management works with the internal audit staff to develop a remediation plan, and internal audit follows up to ensure the plan is timely and effectively implemented.

The plan calls for deficiencies to be prioritized, with remediation deadlines set for each and responsibility assigned to one individual within the business unit.

EXAMPLE

Reporting Deficiencies to the Board

O'Neil & Steenburgen, PLLC is a civil engineering firm. Management periodically creates a report of significant deficiencies and material weaknesses, together with summaries of minor deficiencies and of past deficiencies. These reports are intended to facilitate determination of whether deficiencies are being remedied in a timely fashion, and they are sent to the board of directors for review.

Management has agreed with the audit committee that it will report all deficiencies that are a result of illegal or improper acts, significant loss of assets, or intentional external financial reporting misstatements and omissions, regardless of previous categorization. The audit committee is briefed on causes of reported deficiencies and provides oversight of management's deficiency assessments, actions, and remediation plan progress.

EXAMPLE APPROACHES THAT SMALL TO MID-SIZE ENTITIES CAN USE

Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to determine whether the components of internal control are present and functioning.

- Ongoing monitoring is built into operations throughout the entity and includes explicit identification of what constitutes a deviation from expected control design or performance, thereby signaling a need to investigate both potential control problems and changes in risk profiles.
- Management's ongoing monitoring provides feedback on the effective design and operation of controls integrated into processes, and on the processes themselves.
- Management's ongoing monitoring serves as a primary indicator of both control design and operating effectiveness and of risk conditions.

Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the governing board, as appropriate.

Reports from external sources (e.g., external auditors, regulators) are considered for their internal control implications, and timely corrective actions are identified and taken.

Securities and Exchange Commission Proposal – Internal Control Audits

On May 3, 2019, proposed exempting smaller reporting companies (SRCs) with revenues less than $100 million from the Sarbanes-Oxley Act requirement for independent auditor attestation on management's assessment of the effectiveness of their internal controls over financial reporting.

Although the SEC's goal is to promote capital formation by reducing compliance costs, capital providers and others have expressed concerns about going soft on internal controls and the potential unfavorable results. The potential unfavorable result of going soft on internal controls applies also to private companies.

Following are some of the potential unfavorable results of softening internal control reporting and monitoring:

In April 2012, congress passed the Jumpstart Our Business Startups Act (JOBS Act) to goose the IPO market for small firms. Although company management still needs to disclose management's internal control effectiveness assessment (and any material weaknesses), the Act exempted these companies from external auditors verifying internal control effectiveness.

The SEC reported that entities going public by taking advantage of the JOBS Act had a restatement rate of 13.5%, compared with 8.5% for similar companies that continued with internal control external audits. The SEC did not report the restatement dollar magnitude.

This means that companies with relaxed internal control audits were 1.6 times more likely to restate their financial statements. As a result, while the Act accomplished its goal of increasing the number of companies completing an IPO, the financial reporting quality (and internal control effectiveness) for these public companies decreased.

The Act reduced investor protection. Ultimately, this financial reporting quality reduction could have the opposite effect and discourage capital providers from investing in companies with relaxed internal control monitoring and reporting. Many investors (in public and private companies) may not be comfortable with management having less oversight over company assets. Looser internal controls may cause investors to assess higher company risk which would reduce valuation. Lax internal controls infamously derailed a number of apparently-successful companies, and investors can easily recall examples such as Enron and WorldCom.

Internal control audits differ from financial statement audits. Internal control audits cover financial reporting processes for producing financial information reliability, improving operational efficiency, and complying with internal policies and procedures.

Unit 10

Get Ahead of the Curve on How COVID-19 May Have Infected a Company's Internal Controls

ANTICIPATING INTERNAL CONTROL INFECTIONS

COVID-19 created significant business process, risk, and concomitant internal control changes. One of the most significant changes is transferring employee work locations from the office to remote home locations. This includes accounting and reporting functions.

Beyond the obvious transfer of physical work locations, this transfer impacts how employees work. As a result, companies implemented operations and financial reporting workarounds in a very short timeframe. Many of these processes were designed to be effective in an office environment because they addressed operational and financial reporting risks in a controlled office environment. These processes are not well-suited for a work-from-home environment.

Management is responsible for its internal control design, implementation, and maintenance to achieve the entity's objectives for operations efficiency, compliance with law and regulations, and reliable financial reporting. As a result of COVID-19, certain internal controls may require modification to be effective because significant process changes may have occurred.

Worse, risks have changed, and the existing risk assessment before COVID-19 may be obsolete. Management is also responsible for identifying and mitigating risks.

Change Management

COVID-19 makes evident the importance of a robust change management process. When processes and controls change, management needs to design and implement appropriate controls in response to its post-COVID-19 risk assessment.

Change controls are most critical in legacy or custom information technology systems, but also apply to purchased systems that have decision boxes to check or uncheck. Change controls are effectively a change management process encompassing initiation, approval, the change, testing and validating, user acceptance, and user training.

The danger with ineffective change controls is primarily inadvertent change, versus malicious change or change associated with fraud, which are also risks.

Controls (policies) over change timing are often overlooked and can impact financial statements. For example, changes should rarely occur at critical seasonal peaks which could negatively disrupt operations, nor should changes occur at year end during the accounting close.

Controls (processes) over change include making changes in a text environment, not real-time in a production environment. This may include running parallel (old and changed) applications as a part of the validation step; also, data back-up to avoid losing important operating and supporting documentation. In addition, changes need to be documented.

Change management processes include documenting the reasons for the change, followed by the specific control changes in design and implementation.

Control Environment

All of the following may impact attitudes about financial reporting. COVID-19 and the resulting work-from-home environment have negatively impacted companies' control environment, which provides the foundation for the other internal control components. Among other impacts, this has stressed organizational structures, business and operational processes, execution of authority and accountability.

Not only are financial resources stretched from lower sales volume and higher costs, but also time resources are stressed due to inefficient operations from working remotely. From a control perspective, there may be less experienced employees performing key control activities, and they are following operating and control procedures not designed for remote activity. Thus, the controls implemented are no longer operating as intended.

Management, saddled with resource constraints, may become more tolerant of overriding internal controls. This may also occur because management is focused on other priorities and may more easily overlook control deficiencies. This could produce a relaxed control consciousness and would be dangerous if it became pervasive throughout the organization. "Tone at the top" has an even higher impact than usual with COVID-19. The most dangerous impact is if this relaxed control consciousness spread to infect fraud control effectiveness.

EXAMPLE

Asset impairment is an example of the impact of relaxed control consciousness. Management may evaluate the COVID-19 impact as uniquely "one-off" and containing significant measurement difficulty that management may abandon its established asset impairment assessment procedures. This exacerbates as other employees interpret management's relaxed control consciousness as an indication that circumventing or overriding other internal controls is permissible.

Fraud

Management is required to assess fraud risk separately from operational and financial reporting risks. In just a short time, COVID-19 significantly impacted business processes and the economy's output and employment. While most organizations were hurt by sudden volume shortfalls, COVID-19 rapidly accelerated volume in a few industries. Examples of industries with rapid volume increases are groceries, medical providers, and home-delivery.

This rapid change can increase fraud risk. In companies with rapid volume increases, management may have overridden or employees may have circumvented human resources hiring and employee vetting processes.

In companies with rapid volume decreases, the resulting financial pressure may produce cost-saving measures and business process changes that severely impact control operating effectiveness. Examples are pay reduction and employee layoffs. Fraud risk results from financial pressure on employees, employee changes in justifying certain behaviors, and from a lack of segregation of duties creating fraud opportunity.

Risk Assessment

Organizations are in a risk environment unlike any other management has experienced previously, or that could reasonably be expected to be anticipated. Risk mitigation actions are not familiar, and there is not much prior experience from which to learn.

Management should have already performed a new risk assessment and identified mitigating actions. Examples are for segregation of duties, transaction authorization, and information technology security. Information security is often primary thought of as being hacked. However, information technology security also covers employee system access and transaction authorization and processing, which has increased in complexity from working remotely.

Control Activities

Processes for initiating, authorizing, recording, and processing transactions are different in a work-from-home remote environment. Not only may the pre-COVID-19 processes be different, but also the post-COVID-19 processes most likely lack documentation, approval, and control effectiveness testing.

Processes and controls for adjusting journal entries, making estimates, and accounting judgment for preparing financial statements and financial reporting are now different, not only by being remote but also if staff is now reduced. Financial management needs to document and communicate changes in accounting and financial reporting processes, roles, and responsibilities.

Monitoring Activities

Because COVID-19 may have created many internal control deficiencies, monitoring controls take on increased importance. Examples are new monitoring by analytical review of transactions, authorizations, and processing. Unfortunately, these will primarily be detective controls and not the more desirable preventative controls.

POTENTIAL ACTIONS TO TAKE NOW TO STRENGTHEN INTERNAL CONTROLS

Following are some potential actions to take now because of COVID-19.

1. Reperform a risk assessment

   COVID-19 has placed organizations in uncharted territory that continues to change. Internal controls need to be developed and implemented based on risks and are not "one size fits all" because every organization is unique.

   Risk examples may include: liquidity, solvency, and capital resource availability; debt covenant compliance; and financial and regulatory reporting compliance. Also, information technology security and data integrity.

2. Revaluate existing internal controls

   Some existing internal controls may still be effective, and, if so, need to be validated and documented as implemented and operationally effective, as well as fulfilling the mitigation of risks assessed in step #1. Identify control gaps or internal controls that are no longer effective and need to be replaced.

   Control examples are those that would apply to: a remote work environment, electronic approvals, and electronic documentation.

3. Focus on improving segregation of duties

   Smaller organization have always faced segregation of duties difficulties. Larger organizations, now with a reduced workforce, may not realize that they have segregation of duties deficiencies. Making this more difficult is that executive management may have developed a relaxed control attitude with all of the new challenges presented by COVID-19.

   An example is asset custody. Asset custody was clearer in the pre-COVID-19 environment with most employees physically working in an office. Post-COVID-19 working remotely may make it difficult to separate physical custody, authorization, transaction processing.

4. Document revised processes and internal controls

   Process and control documentation have always been a best practice and required for public companies. Documentation is more critical as risk increases, which has occurred with COVID-19. Critical financial and reporting areas that document the facts, circumstances, as well as the thought processes and rational behind decisions is critical for accounting estimates and management judgment. In a remote less-structured work environment, this may be more difficult to accomplish.

NOTES

Appendix A

ANTI-FRAUD CONTROLS AT THE ACTIVITY LEVEL

In a previous section, the importance of anti-fraud controls as part of the risk assessment process was discussed. Joseph T. Wells, the founder and Chairman of the Board of the Association of Certified Fraud Examiners, the world's largest anti-fraud organization, gave some advice to management. He stated that internal controls are important but they provide only reasonable assurance that fraud will be prevented or detected. There are certain controls that he believes are more likely to help to prevent fraud than others and these are the ones that set the tone for the organization rather than try to detect fraud at the transaction level.

The questionnaire below illustrates some of these controls that could be used by management and the board to assess their anti-fraud programs and controls.[28]

Anti-Fraud Provision	Question	Response
Training	Do employees receive training that helps to educate them about: ■ What constitutes fraud? ■ Have costs of fraud such as job loss, publicity issues, etc., been discussed with employees? ■ Have employees been told where to go for help if they see something? ■ Is there a zero tolerance policy for fraud and has it been communicated?	
Reporting	Does the entity have an effective way for employees to report fraud? ■ Are there anonymous reporting mechanisms? ■ Do employees understand that those issues reported will be investigated?	
Perception of Detection	Does the entity seek knowledge of fraudulent activity? ■ Is there a message sent that that there will be tests made to look for fraud? ■ Are there surprise audits? ■ Is software used to identify issues from data?	

[28] Adapted from Joseph T. Wells' article in the Journal of Accountancy, June 2010.

Anti-Fraud Provision	Question	Response
Management's Tone from the Top	Does the organization value honesty and integrity? ■ Are employees surveyed to determine whether they believe that management acts with integrity? ■ Have fraud prevention goals been set for management and are they evaluated on them as an element of compensation? ■ Is there an appropriate oversight process by the board or others charged with governance?	
Anti-Fraud Controls	Are any of the following performed? ■ Risk assessments to determine management's vulnerabilities ■ Proper segregation of duties ■ Physical safeguards ■ Job rotation ■ Mandatory vacations ■ Proper authorization of transactions	
Hiring Policies	Are the following incorporated? ■ Past employment verification ■ Credit check ■ Criminal and civil background check ■ Education verification ■ Reference check ■ Drug screening	
Employee Assistance	■ Are there any programs in place to help struggling employees – financial issues, drug issues, mental health issues? ■ Is there an open door policy so that employees can speak freely? ■ Are anonymous surveys conducted to assess employee morale?	

Entities should also have anti-fraud programs at the activity level. After a fraud risk assessment is performed, management should consider if the additional specific internal controls would add value, if implemented. Following are examples of internal controls that could help prevent and detect fraudulent activity related to cash receipts, cash disbursements, and payroll in a small to mid-size company.

Controls over Cash Receipts

Internal Controls that Could Help Prevent Cash Schemes: (Small to Mid-Size Organizations)					
Control	**Stealing Deposits**	**Stealing Cash on Hand**	**Skimming Part of Contribution or Sale**	**Kiting**	**Lapping**
Use pre-numbered deposit slips	✓		✓		
Make all deposits intact daily	✓		✓		
Keep un-deposited amounts in a safe	✓		✓		
Consider a lockbox for large volumes of cash receipts	✓	✓	✓		
Use multi-part deposit slips and compare the amount on the in-house copy to the amount deposited on the bank statement	✓		✓		
Perform analytical review on the quantity of cash received from week to week and month to month or for events	✓	✓	✓		✓
Reconcile receivables ledger to the general ledger balance with supervisory review					✓
Bond employees who handle cash receipts and make deposits	✓	✓			✓
Have supervisory personnel review the pledges or other receivables for collectability, as well as any write-offs before they occur					✓
Post a toll free number where donors, customers, or clients can make complaints	✓		✓		✓
Separate the responsibility for logging the cash receipt, posting the cash receipt, and depositing the cash receipt (to revenue or against receivables)	✓		✓		✓
Have employee that is independent of billing, posting receipts, and cash handle any complaints from donors, clients, or customers	✓		✓		

Have independent supervisory personnel perform tests at the end of the period to determine if any interbank transfers have been properly recorded				✓	
For events or times where there is a large amount of cash collected, have two people count cash as a check on one another	✓	✓	✓		

Controls over Cash Disbursements

Internal Controls that Could Help Prevent Fraudulent Disbursements (Small to Mid-Size Organizations)

Control	Kick-backs	Fictitious or Inflated Invoices	Excess Purchasing Schemes	Duplicate Payment Schemes	Stealing Checks	Stealing Cash by Using Wire Transfer
Use competitive bidding	✓		✓			
Review recent purchases to see whether one vendor is winning the majority of bids	✓					
Notify vendors of conflict of interest policy	✓					
Scan general ledger for unusual levels of purchases		✓	✓	✓		
Use data extraction software to search for vendors with same addresses as employees, vendors with P.O. boxes, duplicate payments		✓	✓	✓		
Use programmed controls to prevent unauthorized access to check writing and AP systems		✓	✓		✓	
Use pre-numbered requisition, purchase orders, receiving reports, and ensure sequence is accounted for		✓	✓	✓	✓	
Reconcile subsidiary ledgers to G/L		✓				

Internal Controls that Could Help Prevent Fraudulent Disbursements
(Small to Mid-Size Organizations)

Control	Kick-backs	Fictitious or Inflated Invoices	Excess Purchasing Schemes	Duplicate Payment Schemes	Stealing Checks	Stealing Cash by Using Wire Transfer
Perform analytical review on expenses by category		✓	✓	✓	✓	✓
Scan G/L for unusual activity		✓	✓			
Lock up check stock		✓			✓	
Set up positive pay with bank		✓		✓	✓	
Use multipart / pre-numbered checks		✓				
Investigate void or reissued checks		✓				
Recompute vendor invoices for accuracy		✓				
Match vendor invoices with requisitions and receiving documents		✓				
Require varying levels of approval for higher purchases		✓				
Use approved vendor list and have management approve changes to master file		✓		✓		
Enforce mandatory vacations	✓	✓	✓	✓	✓	✓
Look at returned checks or electronic bank copies to see if there is anything unusual about payee, endorsement, or authorized signature	✓					
Compare budget to actual disbursements		✓	✓	✓		
Require original invoices and receiving reports				✓		
Use passwords for those initiating and those authorizing wire transfers						✓

Internal Controls that Could Help Prevent Fraudulent Disbursements (Small to Mid-Size Organizations)

Control	**Kick-backs**	**Fictitious or Inflated Invoices**	**Excess Purchasing Schemes**	**Duplicate Payment Schemes**	**Stealing Checks**	**Stealing Cash by Using Wire Transfer**
Require bank to call back to verify wire transfers over a certain amount						✓
Compare petty cash reimbursements to other reimbursements to prevent double dipping by employees				✓		
Bond employees	✓	✓	✓	✓	✓	✓
Bank statement sent to senior management or someone who does not have responsibility for cash receipts and disbursement records	✓					
Reconciliation of bank statement by someone who doesn’t prepare or sign checks or initiate wire transfers		✓			✓	✓
Have an independent person review bank reconciliation		✓			✓	✓
Separate duties for person who authorizes invoices for payment and person who receives vendor refunds				✓		
Separate duties between those who initiate, process, authorize, record, and handle check stock and check writing		✓	✓	✓	✓	
Separate duties between those initiating and approving wire transfers						✓
Separate purchasing from requisitions and receiving	✓					

Controls over Cash Payroll

Internal Controls that Could Help Prevent Payroll Schemes (Small to Mid-Size Organizations)

Control	Fictitious Employees	Inflated Payroll	Terminated Employees on Payroll	Expense Report Fraud	Stealing Checks	Payroll Tax Schemes
Use a payroll service and have senior management review payroll documentation analytically	✓	✓	✓		✓	
Payroll service handles payroll tax payments to IRS						✓
Supervisory approval for additions and terminations	✓		✓			
Supervisory review to changes in the master payroll file	✓		✓			
Surprise delivery of paychecks if not direct deposited	✓					
Mandatory vacations for personnel and payroll employees	✓	✓	✓		✓	
Supervisory approval of time sheets or time cards		✓				
Lock personnel files	✓					
Lock up payroll check stock					✓	
Reconcile payroll with the general ledger			✓			✓
Reconcile total W-2 wages to the general ledger and payroll register			✓			✓
Require employees to sign W-4 forms and other appropriate withholding documents						✓

Internal Controls that Could Help Prevent Payroll Schemes
(Small to Mid-Size Organizations)

Control	Fictitious Employees	Inflated Payroll	Terminated Employees on Payroll	Expense Report Fraud	Stealing Checks	Payroll Tax Schemes
Use direct deposit	✓		✓		✓	
Separate duties of check stock custody and check signing	✓		✓		✓	
Separate duties for preparing payroll and personnel					✓	
Use a separate imprest account for payroll and deposit only the amount needed		✓			✓	
Senior management performs analytical review of payroll and payroll liabilities	✓	✓	✓		✓	✓
Supervisory employee reviews reimbursable expenses against budget				✓		
Establish travel, hotel, and meal guidelines and limits				✓		
Require review and approval of all expense reports before they are paid. Check signers should not approve their own reports				✓		
Require that original receipts be submitted for each item over a certain dollar threshold				✓		
Review mileage reimbursements for reasonableness in accordance with expectations				✓		

EXAMPLE

The owner of a small retail operation was concerned about the cost of inventory which appeared to be high compared to her expectation. To prevent fictitious invoices or inflated invoices, her auditor suggested the following controls:

- Owner scans the general ledger for unusual levels of purchases or unfamiliar vendors
- Management periodically uses data interrogation software or Excel to run a search for vendors with the same address as employees, duplicate payments, and vendors that have addresses that are post office boxes
- Pre-numbered purchase requisitions and receiving reports are used and reconciled to determine if all numbers were accounted for and unused documents were properly void
- Owner performs analytical review on expenses
- The entity locks up its check stock
- Owner periodically scans the bank account online for unusual debits since fraud is committed electronically by people who have access to the entity's bank account information.
- Management compares budget to actual and investigates discrepancies

EXERCISE 4 – KEY ACTIVITY CONTROLS

Instructions: Following is a narrative on the payroll in a small company. Following the narrative is a list of controls. These are noted in the narrative by number in the places in the process flow where the controls occur.

1. Read the narrative and the controls and identify the key controls. Bear in mind that the controls that come from the CX 5 series are generic in nature and in this narrative have been modified to fit the client's circumstances.

2. Find the deficiencies or "holes in the controls" which would need to be evaluated to see if they are significant deficiencies or material weaknesses (discussed later in the manual).

Note that this exercise is for discussion purposes only. There is no right answer. Auditors will identify as many controls as key controls as they need to in order to feel comfortable.

The management of a retail chain of vitamin stores prepared the following assessment of the entity's internal controls.

Detailed System Documentation – Payroll Process

The Company has a weekly payroll that consists of both salaried and hourly employees. The work week runs from Sunday through Saturday. With the exception of the CEO, all employees use a "swipe card" to record their hours **(10)**. Store Managers have access to the ADI time card system and check their employees' hours prior to the payroll being processed**.** During the year, the week's payroll is recorded in the month in which the Saturday which closes the pay week falls. Accrued payroll is only recorded at year end.

Most employees are paid by direct deposit. Those who decline direct deposit or don't have a bank account are paid by check. Payment of wages in cash is prohibited **(9).**

There are two processes to prepare payroll:

- As stated above, all employees except the CEO use a swipe card to record their arrival at and departure from work. These swipes are recorded via hardware and software purchased from ADI Time, a nationally recognized company based in the area. A computer in the accounting office polls the time clocks at night to collect the day's swipes (see the processing procedure below to handle missing swipes). As discussed in greater detail below, at the end of the pay week, the Payroll Coordinator prepares the payroll for submission to the outside payroll service provider.

- An outside service provider, **(1)** processes the payroll at their Warwick, RI facility once the input has been received (weekly, either on Monday or Tuesday) from the Payroll Coordinator. The processed payroll is returned to the Payroll Coordinator the following day and she reviews to ensure that the processing is complete.

The Payroll Coordinator prepares the documentation to send to the payroll service for processing.

- On Monday morning, the Payroll Coordinator checks the time system to ascertain there are no missing punches (an employee may forget to punch in or out on their shift). A Missing Punch report is generated and reviewed. Salaried exempt employees are only required to punch once a day. The Payroll Coordinator will enter the second punch. The report is re-run to determine any additional missing punches. The Payroll Coordinator will check for missing punches again around noontime. If there are still missing punches, the appropriate Supervisor or Store Managers are notified to correct their employees' hours. Note: the Store Managers or their designee has access to ADI to view their own employee's time records. This access is password protected and only gives them access to this section of ADI and only their own store. The managers are not able to make any changes other than time worked. The Managers can make changes to the time records from their computer stations. Time changes due to a missed punch are based on a Supervisor's personal knowledge of the employee's starting or ending a shift, by reference to the daily work schedules or a "paper time card" that the employee completes and gives to the Supervisor. Any changes made by a Manager are shown in red on the Payroll Coordinator's screen. The Managers check the time cards at various times during the week, but have been requested to have the final weekly review done prior to noon on Monday.

- The HR manager and the CFO get a weekly overtime report from the Payroll Coordinator for their review.

- The Human Resources Assistant enters all vacation, sick, and personal time in the ADI Time software. All employees are required to complete a Leave Request Form for any time away from work. This form is approved by the employee's Supervisor (or Store Manager if the Supervisor is unavailable) and given to the Human Resources Department for processing.

- The Human Resources Manager checks the leave requested on the Leave Request Form against the report generated Fringe Benefit Hours Report (lists available leave time by employee and store) generated by the service bureau. This report is part of the payroll package that the Payroll Coordinator receives with each payroll that is processed. The HR Manager signs off on the Leave Request Form and gives a copy to the HR Assistant. This copy is used as a basis for entering the data into the ADI Time software. When all time off and punches are complete, the data is uploaded to the Payroll Software (uploaded to service organization) for further processing as described below.

- Once the ADI Time data is uploaded to Payroll Software, any necessary payroll adjustments are made. This includes mileage reimbursements (Mileage Reimbursement Form is completed and approved by the employee's supervisor) and retro hours, is e-mailed to the Accounting Manager and Payroll Coordinator. The CFO is also notified of mileage and adjustments being made so that the payroll budget can be adjusted to eliminate budget variances. Notification for wage increases, employee additions or deletions, changes in employment status, eligibility for health benefits, etc., are received from the Human Resources Manager **(2)**. The Payroll Coordinator enters the changes, signs off on the paperwork, and returns the paperwork to the Human Resource Assistant. The Human Resource Assistant checks the input to PeopleTrak, the HR personnel database, to ensure that all the changes have been made **(1)**. After balancing the payroll input worksheet to the ADI printout of hours worked by category, the Payroll Coordinator closes the current payroll and sends it (on-line) to the service organization.

- Payroll is returned the next day by a service organization courier. Part of the data returned is a CD, which has the Payroll Register, and other related payroll reports. The CDs are saved on the Payroll Coordinator's computer and the original is destroyed. The Payroll Coordinator prints the last page of the payroll register and compares totals to the weekly payroll summary worksheet and the Gross to Net report **(3)**. Store Managers are given a Fringe Benefit Report that shows vacation, sick, or personal time off during the current week, year to date, and remaining time. A listing of payroll checks is given to the Accounting Manager for use in the bank reconciliation process.

- The CFO or Accounting Manager is notified of the dollar amount of payroll so funds can be transferred into the bank account. The Payroll Coordinator prints a copy of the Gross to Net Calculation Report prior to closing the weekly payroll. The Accounting Manager checks the amount per this report with the deduction per the bank **(3)**.

- The journal entry to record the payroll is e-mailed to the Payroll Coordinator by the service bureau. It is downloaded into the MAS 200 accounting system and reviewed by the Payroll Coordinator prior to posting to the General Ledger. The Payroll Coordinator also receives a file for the TIAA-CREF 403(b) contribution withholdings. The Payroll Coordinator then sends the file to TIAA-CREF on-line. Payment is made at this time by an EFT transfer through Bank Left Standing and a journal entry is made to record the EFT in the General Ledger. The Accounting Manager reviews the posted journal entry and verifies the amount to the deduction from the bank account to the payroll records.

The payroll is funded through a separate bank account **(4).** Funds to cover the payroll are transferred to the payroll account from one of the other Company operating accounts. The Payroll Coordinator or the Accounting Manager makes a journal entry to record the transfer. The Accounting Manager reviews entries made by the Payroll

Coordinator. A printout of the bank transfer transaction is attached as supporting documentation.

The payroll tax returns are prepared and filed, and deposits of withholdings are made by the payroll service bureau. Copies of the payroll tax returns are sent to the Payroll Coordinator. They are then given to the Accounting Manager for review prior to filing them in the Finance Office. As part of the year end audit process, a reconciliation of W-2 wages to amounts recorded in the General Ledger is prepared **(5)**.

Every month, the CFO receives from the service bureau an Excel spreadsheet with the month's payroll activity in complete detail. Every employee's pay, separated into complete component parts, is in the spreadsheet. For example, if an employee worked in different stores during the month, there would be separate lines in the spreadsheet detailing that employee's pay by store. If that employee had overtime, his or her pay is further separated into regular and overtime, again by charged store. Sick time, vacation, retro hours, weekend premium, is all separated out, again by charged store. The CFO imports each month's Excel payroll file into an Access database. When the CFO prepares a month's financial statements and finds discrepancies between budgeted and actual payroll for a given store, the CFO is able to determine from the Access database every element of full- and part-time pay for that store, and compare it to budget and follow up on variances **(8)**.

The payroll accrual is made at the end of the year. The Accounting Manager determines how many days of payroll need to be accrued and prepares a worksheet as the basis for the adjustment, obtains the CFO's approval, and prepares the journal entry **(6)**.

Vacation Pay Accrual

The vacation pay accrual is adjusted at year end. The CFO prepares a worksheet that lists employees by store, the amount of vacation time due them, the rate of pay, and extended dollar value. The CFO computes the change from the previous year's accrual by store, and prepares a journal entry. The journal entry is given to the Accounting Manager to review. If the Accounting Manager believes there is a problem with the calculation, he reviews it with the CFO. Otherwise, he posts it to the General Ledger. A copy of the journal entry and worksheet is then filed in a binder **(7)**.

During the year, if an employee leaves the Company any accrued vacation pay they receive is deducted from the Accrued Vacation account so as not to distort the weekly payroll amounts.

Segregation of Duties

Initiating Transaction	Cash Handling	Posting Transaction	Supervision and Monitoring
HR function handles terminations and additions and requests for vacation and other time off. Time clock (automatic control)	CFO releases cash to the interest account but cash is mainly distributed electronically by the	Payroll Coordinator.	Payroll Coordinator reconciles input to the payroll system with the output that they deliver. The CFO reviews the payroll for funding. The Accounting Manager

feeds into CSC. This is also reconciled. Store managers review payroll for their stores. Payroll Coordinator sends information to the service organization.	service bureau. There are very few manual checks.		verifies that the amount per payroll is what is deducted from the bank. The Accounting Manager reviews the journal entry that the Payroll Coordinator will post. The HR Manager and the CFO get a weekly overtime report from the Payroll Coordinator and review it. Payroll is analytically reviewed and makes up part of the board package.

NOTE: A service bureau is used to process payroll. At this time, there is no SSAE 18 report for the service bureau. However, due to the extensive monitoring that occurs, this is not deemed to be a significant deficiency by management. SSAE 18 states that if the controls are resident at the entity, a service auditor report is not necessary.

Internal Controls

1. An outside vendor is used for payroll processing. Store Managers monitor the input prior to payroll processing. Additions to and terminations from the payroll are checked by the Human Resource Assistant. **(Completeness, occurrence, valuation)**

2. All changes to the payroll input are approved by a person independent of accounting. **(Occurrence, completeness, valuation)**

3. The Payroll Coordinator reviews the summary output from the service bureau for accuracy. The Accounting Manager compares the amounts per the Gross to Net calculation to the amount deducted from the payroll bank account. **(Accuracy, existence, occurrence, completeness, valuation)**

4. Transfer and reconciliation of payroll costs to a separate payroll account is a control that the amount of payroll per the payroll department equals the amount of payroll per the service bureau. **(Occurrence, completeness)**

5. Payroll tax filings are reviewed by the Accounting Manager. A year end reconciliation of W-2 wages to the General Ledger is made. **(Existence, occurrence, completeness, cutoff, accuracy)**

6. Only one payroll accrual is made, at the end of the year. The Accounting Manager determines how many days of payroll need to be accrued and prepares the adjustment. The CFO reviews the accrual worksheet journal entry. **(Existence, completeness, cutoff, valuation)**

7. The vacation pay accrual is adjusted at year end. The CFO prepares a worksheet that lists employees by store, the amount of vacation time due them, the rate of pay, and extended dollar value, computes the change, by store, from the previous year's accrual, and prepares a journal entry. The worksheet is given to the Accounting

Manager for his review and if in agreement for posting to the General Ledger. **(Existence, completeness, cutoff, valuation)**

8. Analytical review is performed monthly by the CFO and this information is put into the package that is reviewed by the board. **(Existence, occurrence, completeness, accuracy)**

9. Payment of wages in cash is prohibited. **(Existence, occurrence)**

10. Adequate timekeeping and attendance records are maintained. **(Accuracy, classification)**

EXERCISE 5 – KEY ACTIVITY CONTROLS AT HOWARD ELECTRONICS

Howard Electronics

Howard Electronics was introduced in a previous section. Jon and his brother Paul (CFO) have asked you to review the documentation that Janet, the accounting manager, put together on the sales and accounts receivable system (sales of merchandise only).

The following employees play a role in that system:

- Janet – accounting manager

- Jennifer – accountant responsible for billing and cash receipts

Some of the company's sales at the retail store are by cash or credit card. However, most sales are to customers on account. The merchandise is picked up at the warehouse but the customers are billed. There is no shipping.

When a customer comes in to purchase electronic office equipment, the sales person generates an invoice listing out the goods. These invoices are pre-numbered. A copy is maintained in a file and a copy is given to the customer to take around to the pickup window. The warehouse employee stamps the invoice and has the customer sign that the goods were picked up. At the end of the day, the stamped and signed invoices are sent to accounting. The sales person sends the other copy to accounting with the register tape and the cash/checks/credit card slips for the day. The sales person prepares a report that reconciles the total sales from the register with the amount to be recorded as receivable plus the cash/checks/credit card slips.

The accountant prepares a deposit slip for the cash and checks and enters in all of the sales, with corresponding entries to cash or receivables.

On the last business day of the month, the accountant bills the customers on account.

Mail comes in and is opened by the receptionist. She bundles all of the checks and supporting documentation together and gives it to the accountant. The accountant posts the incoming cash to the receivables ledger. The checks are stamped and a deposit slip is prepared. The accountant gives the deposit slip to the accounting manager who makes the deposit at lunchtime each day. The deposit consists of the cash and checks from the previous day's cash sales and the payments on account.

On the 15th day of the month, the accountant runs an aging report and follows up on overdue invoices. Periodically, the CFO writes off uncollectible accounts.

At the end of the month, the accountant reconciles the bank account and the accounting manager reviews the reconciliation. The company has a budget that is prepared by the accounting manager and approved by the CFO. Every month, the CFO reviews a report prepared by the accounting manager that compares budget to actual for sales of the various products, as well as the repair invoices.

1. Are the internal controls over sales and accounts receivable properly designed?

2. How would you determine if they had been implemented?

3. Do you have any suggestions for Jon and Paul to improve internal controls over cash, given the personnel available?

Appendix B

SMALLER ENTITY INTERNAL CONTROLS

The COSO framework does not provide a definition of smaller entities in terms of revenues, assets, or capitalization. It provides some characteristics that may indicate a smaller entity. When these characteristics are present, the board and management should expect different challenges to implementing effective internal controls.

Characteristics of a smaller entity:

- Few lines of business and fewer products within lines
- Concentration of marketing focus by channel or geography
- Leadership by management with significant ownership interest or rights
- Fewer levels of management with wider spans of control
- Less complex transaction processing systems
- Fewer personnel having a wider range of duties
- Limited ability to maintain deep resources in line as well as support staff positions such as legal, human resources, accounting, and internal auditing

These characteristics may cause management to view internal controls as an "add on" rather than an integral part of business processes. Major challenges for small entities are:

- Adequate personnel to segregate duties.
- Management's ability to dominate activities and override the system because they have the ability to control the activities of others and the board does not serve as a challenge on their actions. Therefore, it may appear that business performance objectives have been met when, in fact, controls have been circumvented.
- Obtaining independent, outside parties with financial and operational expertise to serve on the board of directors and the audit committee.
- Obtaining qualified accounting and compliance personnel with sufficient experience and skill.
- Lack of time and focus on internal control due to other pressing business demands.
- Controlling information technology (IT). Frequently, smaller entities place extensive reliance on one IT professional because others in the entity do not understand technology.

These challenges do not mean that internal controls are nonexistent, not effective, or cannot be improved. It means that the entity may need to be creative in finding ways to mitigate these deficiencies.

One big challenge for small to mid-size entities is striking the balance between **formal controls** and **informal controls**. Where formalization provides structure and helps others in the organization to understand the various roles and responsibilities, formalization can be burdensome. On the other hand, informal controls are more difficult to apply on a consistent basis because they are not a documented part of a routine.

EXAMPLE

A small retail company has five shareholders who are all on the board of directors. Management consists of a President, Chief Financial Officer, Operations Manager, Accounting Manager and 3 accounting staff. Management is directly involved in all decision making that relates to the reliability of financial reporting. Board meetings are not regularly scheduled and when held consist of discussions of operations topics. Analytical procedures are performed on the financial statements by senior management on at least a monthly basis. The financial statements are reviewed with the board once a year. Risk is discussed among senior management but the discussion is not documented.

Although management and the board value accurate information and accountability, the company does not have a conflict of interest policy or code of conduct. Everyone assumes that management and the employees are honest. Entity level controls are not formally documented because there are so few people in the company. Without clear guidelines and expectations set by management, conflicts of interest are more likely to arise. Employees may rationalize their behavior saying that they were not aware of any policies.

Sometimes it may appear that the control environment and monitoring components are well designed. The deficiency may be in implementation. Therefore, in understanding these very important components, especially as they are deemed to be factors in mitigating the lack of segregation of duties, the competencies of those individuals performing the controls must be considered.

EXAMPLE

A small governmental entity had a board that appeared to be functioning very well. The minutes of meetings were very descriptive and it was clear that the board spent a significant amount of time evaluating the budget to actual and current period to prior period fluctuations. The board members asked questions of management. However, even with that level of involvement, one year an independent third party was sitting in on a meeting and in a meeting noted that one line item appeared to be particularly high. He asked a question about why it was so high and the board asked management to investigate.

Upon investigation, the board learned that the bookkeeper was stealing and putting the charge in that line item. The dollar value of that line item had not fluctuated in years so the board did not think to ask any questions about it. Over seven years, the bookkeeper stole $1.8 million by creating a fictitious vendor and approving the invoices. Even though the board appeared to be very contentious, they did not have an adequate understanding of the entity's internal controls (lack of a master vendor list, lack of adequate procurement policy requiring bids) or how to properly perform analytical procedures (expectations are important when performing analytical procedures).

Segregation of Duties

Although segregation of duties is technically an activity level control, the controls that may be put in place to help mitigate management's inability to properly segregate duties are at the entity level.

An entity should segregate duties among personnel in order to ensure that no one person has control over two or more phases of a transaction or operation. Segregation of duties reduces the opportunity to perpetrate and conceal errors or fraud in the normal course of employee's assigned functions.

EXAMPLE

If one person processes sales, they should not have access to cash receipts, should not reconcile the bank account, or have the ability to "write off" accounts receivable.

In segregating duties, an entity may utilize people in and out of the accounting and financial reporting area, as well as people on the board of directors. Some not-for-profits use volunteers; this may be risky in that volunteers may not use the same care in performing duties as employees would. And as discussed above, people may be able to perform tasks but do they actually know what they are looking for as they perform them.

Management should segregate duties, to the best of their ability, given the personnel at hand. This is an important place for management to perform a GAP analysis.

Step 1: Identify where the lack of segregation of duties is present. The diagnostic tool below could be used for this purpose.

Segregation of Duties Diagnostic

Fill in the names of the people who perform the following functions:

Expenses and Cash Disbursements

Initiating Transaction	Cash Handling	Bank Reconciliation	Authorizing Transactions	Posting Transaction	Supervision and Monitoring

Vendor Activity

Person responsible for updating the vendor master file	
Person responsible for requesting and processing vendor refunds	

Wire Transfers and Other Electronic Payments

Authorizing Transactions	Initiating Transaction	Confirming Transaction	Posting Transaction	Bank Reconciliation	Supervision and Monitoring

Revenue and Cash Receipts: include information by revenue source

Initiating Transaction – Billing	Cash Handling	Bank Reconciliation	Access to Cash for Electronic Transactions	Posting Transaction	Supervision and Monitoring

Payroll

Initiating Transaction	Payroll Master File	Authorizations	Changes in Pay Rates, Withholdings, Benefits, etc.	Posting Transactions	Supervision and Monitoring Including Output of Service Provider

Journal Entries

Person responsible for initiation of journal entries	
Person responsible for approval of journal entries	

EXERCISE – SEGREGATION OF DUTIES

Jenny and Jim own a small service company that repairs computers. Jim has another full-time job and Jenny has a 20-hour-a-week part-time job so they rely on the services of a bookkeeper and one other administrative person. The bookkeeper works in the office on accounting and related tasks and the administrative person assists but primarily takes orders and schedules repairs either in the shop or at a client's place of business. There are two repair people. The company requires payment at the point of service except for two corporate customers so there is very little billing. Most of the payment for services is on site and customers generally use credit cards although sometimes the repair people will receive a check at the client site. Both cash and checks are used for payment at the repair facility.

The company maintains an inventory of parts that are typically used in repair but other items are ordered to meet repair needs.

INSTRUCTIONS

Using the segregation of duties diagnostic, propose a segregation of duties plan for Jenny and Jim's repair business. Personnel include:

- Bookkeeper – Assume that the bookkeeper is full time (40 hours)
- Administrative person – Assume that the administrative person spends 30 hours a week on taking orders and scheduling and has 10 hours to spend on other tasks

- Non-accounting personnel such as repair personnel could be trained to perform some of the less technical duties

- There is no governing board

- Owners (Jim and Jenny)

TASKS

1. Record sales & receivables

2. Write checks

3. Sign checks

4. Reconcile bank statement

5. Record expense transactions

6. Approve payroll to send to payroll service provider

7. Disburse petty cash

8. Authorize purchase orders

9. Authorize check requests

10. Authorize invoices for payment

11. Review bank reconciliations

12. Sign important contracts

13. Make compensation adjustments

14. Receive and open bank statements

15. Mail checks

16. Complete deposit slips

17. Make deposits

18. Perform interbank transfers

19. Prepare invoices

20. Review petty cash

21. Approve vendor invoices

22. Perform analytical procedures

23. Initiate journal entries (including to record payroll)

24. Authorize journal entries

25. Open mail and log cash

26. Periodically count the inventory on hand

Bookkeeper	Administrative Employee	Repair People	Owners

Compensating Controls

Smaller entities can also use compensating controls to help mitigate deficiencies caused by the lack of the ability to segregate duties.

EXAMPLE

A small distribution entity had insufficient personnel to properly segregate duties, resulting in a risk that a sales person could sell goods at little or no charge to customers and record the understated charge in the accounting system. Then they could receive a kickback or simply collect more money and not remit it to the entity. If the owner/manager performed a reconciliation of changes in inventory on hand with sales reported by the sales person, it would become apparent that there was a discrepancy. In addition, the owner/manager could review the price per unit sold to see if it was consistent with the price list and follow-up on significant discounts.

Following are examples of other compensating controls that can help a small entity mitigate its lack of ability to segregate duties:

Compensating Control	How it Works
Review of reports of detailed transactions	Management reviews reports of detailed transactions to identify errors or fraud. In the sales example above, the manager would consider the transaction date, customer description, dollar amount, and any offsetting account (i.e., discounts).
Review sample of transactions	Management selects a sample of transactions that are chosen from a system generated report or data query program. Data extraction software could also be used to choose transactions. The review would consist of the transaction date, customer description, dollar amount, and any offsetting account (i.e., discounts).
Periodic counts of assets and reconciliation with accounting records	Management would periodically count sections of inventory and compare it with inventory records, investigating differences.
Review budget analysis and cost trends	This may be the least effective of these techniques if small thefts or errors.

The issue becomes, "Is management going to consistently perform the monitoring function?" If the monitoring function is consistently applied, the lack of segregation of duties is less important because the monitoring is a compensating control. If it is not consistently applied, then errors or fraud could remain undetected.

Consistent performance of these techniques will also send a message to employees that management cares about asset accountability and will take action against employees who commit fraud. As it relates to errors, it will send a message to employees that care in performing duties is important.

Management Override

Smaller businesses and not-for-profit organizations may have one strong individual who dominates the entity, has a great deal of discretion, and provides personal direction to employees. Sometimes this is due to the size of the organization and sometimes due to the fact that they either own the business, or in the case of not-for-profit organizations, have a strong personality and believe that they know what is best for their constituents.

On one hand this can be helpful because that person has significant knowledge of the entity's processes, operations, policies and procedures, contractual obligations, and generally has a good handle on the entity's risks. But there is a downside.

With this situation there is a high possibility that management could override controls. Clearly, the best guard against this is a strong committed independent board of directors that will challenge the chief executive on issues of financial accountability and accurate financial reporting. However, in closely-held companies, this is not likely to be the case making the prevention of management override very challenging.

Following are some ways that there is potential for management override:

- Instill and maintain a corporate culture that focuses on and stresses the need for integrity and ethical values. This can be supported and reinforced through recruiting, compensating and promoting people where the values are reflected in their behavior.

- Implement and maintain an effective audit committee chair. Whistleblowers should have direct access to the audit committee chair or a board member (depending on whether the entity has an audit committee).

There are some very inexpensive services that will establish and monitor a hotline for people to call. Fraud studies have shown that if employees believe in the ethics and integrity of the entity, they are more likely to report suspicious behavior and less likely to commit fraud themselves. Of course, to accompany the whistleblower program, is a commitment to follow up on issues and to punish violations, no matter how high the person may rank in the entity.

Note that the cost of anonymous reporting vehicles such as hotlines have come down over the past several years. Companies such as Ethics Point, Allegiance, and Lighthouse provide hotline solutions and other assistance to entities based on the number of employees and services needed.

Attract and retain qualified members for the board. The **audit committee** or equivalent should be comprised of knowledgeable independent individuals who are not reluctant to challenge management on issues that arise. They should meet privately with the external auditor. The board should thoroughly understand the entity and be able to identify activities that would have an impact on financial reporting.

If the entity is large enough and can afford it, an internal audit function that reports to the audit committee would be an excellent mitigating control.

Smaller entities may want to consider the following:

- Instead of a hotline, a designated board member could field calls or even emails. The purpose of the anonymous reporting vehicle is to send a message to employees that their concerns are important. It gives them an outlet to report any suspicious behavior and helps to overcome the presumption of inappropriate management override if the system is effective.

- Add a financial expert to their boards, if they believe an audit committee is not needed. A financial expert would be important if management does not have the skills to prepare its own financial statements. That person could be called upon to assist. It is important to remember that the smaller the management team, the more difficult it is to overcome the presumption of inappropriate management override, especially if the persons are related. An entity may want to contact the state society of CPAs to determine if there are any willing CPAs to serve on boards. Many states have a **Center for Nonprofits** that will assist not-for-profit organizations in finding board members.

Qualified Accounting Personnel

Sometimes smaller entities have a difficult time attracting and retaining qualified accounting personnel who understand and can implement generally accepted accounting principles, understand the intricacies of financial reporting, and have the ability to draft financial statements and disclosures. In many cases, these entities have relied heavily on their external auditors to provide them with advice and expertise in this area. External auditors of non-public entities, except those who are required to report under Government Auditing Standards,[29] can still assist management with these functions.

However, this circumstance may result in an AU-C 265 comment. AU-C 265 notes that if the entity lacks controls over the selection and application of accounting principles that are in conformity with GAAP (or a special purpose framework if that is the case) this may be a significant deficiency.[30] AU-C 265 provides significant deficiency examples. This involves the entity having enough expertise in selecting and applying the accounting principles.

Another circumstance that could result in an AU-C 265 comment is the lack of qualified personnel in the accounting and reporting function. This involves being able to properly apply GAAP and prepare financial statements, including footnotes. This essentially means the entity does not have someone who has the skills to prepare the financial statements, including notes. Note: There would be no significant deficiency or material weakness if the company outsources the preparation of financial statements to their auditors, as long as the company has personnel with the skills to review the statements, fully understands them, and take responsibility for them, including whether the disclosures are complete. The auditor would determine if this deficiency would be considered a deficiency in internal control, a significant deficiency, or a material weakness. To prevent AU-C 265 comments, it may be advisable for companies to seek this advice from someone other than an external auditor. **No matter who is consulted, entity personnel still need to have enough expertise to make their own decisions based on external advice.**

Banking Controls and Other Outsourcing

Banking controls and the outsourcing of transaction processing to third parties can help to mitigate a lack of segregation of duties.

Monitoring Activities

Monitoring activities can be performed by management or by the board. It is important that they are performed thoroughly and with the knowledge of what to look for. Sometimes people who start small businesses, executive directors of nonprofits and board members may have significant content knowledge related to the entity but know little about accounting processes and internal controls. A well-designed control performed by someone who doesn't really understand it is not effective.

[29] Under GAAS, the auditor is able to draft financial statements, including footnotes, but is not able to implement accounting principles for them. The auditor can always provide advice and give management tools and templates to use.

[30] AU-C 265 does not provide examples of circumstances that are ordinarily considered significant deficiencies.

Take Advantage of Diversified Learning Solutions

We are a leading provider of continuing professional education (CPE) courses to Fortune 500 companies across the globe, CPA firms of all sizes, and state CPA societies across the country, as well as CPA associations and other financial organizations. Our efficient and flexible approach offers an array of customized cutting-edge content to meet your needs and satisfy the priorities of your business. Select from live classes, live webinars, conferences, or online training, including Nano courses, based on your preferred method of learning.

Meet your CPE requirements, increase productivity, and stay up-to-date with relevant industry trends and mandatory regulations with collaborative live or online learning.

Live Training Topics	Online Training Topics
Accounting and Auditing	**Accounting and Auditing**
Employee Benefit Plans	**Business Law**
Ethics	**Business Management and Organization**
Information Technology	**Economics**
Governmental and Not-For-Profit	**Ethics**
Non-Technical (including Professional Development)	**Finance**
Tax	**Information Technology**
	Management Services and Decision Making
	Personal and Professional Development
	Tax

> "We have enjoyed [your] programs and have found the content to be an excellent learning tool, not only for current accounting and management issues, but also how these issues apply to our company and affect how our business is managed."
>
> **—Debbie Y.**

KAPLAN®

www.kaplanfinancial.com | 332 Front Street South, Suite 501, La Crosse, WI 54601 | 800.824.8742