



Lynn Fountain  
Consulting and Training

# BEST IN CLASS INTERNAL CONTROLS: BEST PRACTICES FOR FINANCE PROFESSIONALS

LYNN FOUNTAIN, CPA, CGMA, CRMA, MBA

[WWW.LYNNFOUNTAIN.NET](http://WWW.LYNNFOUNTAIN.NET)

FOUNTAINLYNN1@GMAIL.COM

# INTRODUCTION

- Internal controls are defined as the mechanisms, rules, and procedures implemented by a company to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud.
- Internal controls is a means by which an organization's resources are directed, monitored, and measured.
  - This includes operational and compliance activities.
  - It plays an important role in preventing and detecting fraud and protecting the organization's resources.

---

# AGENDA

- 
- Identify key principles of effective internal controls and risk management.
  - Evaluate best practices for implementing internal controls in financial operations.
  - Assess internal control frameworks, including COSO and other industry standards.
  - Develop strategies to enhance monitoring, documentation, and reporting of controls.

---

# KEY PRINCIPLES OF EFFECTIVE INTERNAL CONTROL AND RISK MANAGEMENT

# KEY PRINCIPLES OF EFFECTIVE INTERNAL CONTROL AND RISK MANAGEMENT

- Internal control is affected by an organization's structure, work and authority flows, people, and information systems, and is designed to help the organization accomplish specific goals or objectives.
- A small organization with limited resources may not be able to segregate duties with the same rigor that a larger organization can.
  - However, that does not give small organizations an excuse to ignore the importance of that control.
  - They must find other ways to mitigate potential issues.

# KEY PRINCIPLES OF EFFECTIVE INTERNAL CONTROL AND RISK MANAGEMENT

- Internal control is part of an organization's overall responsibility and required due diligence to ensure its operations are effective.
  - Management is the “keeper” and “inventor” of internal controls and must take ownership.
- A key concept of internal control is that even the most comprehensive system of internal control will not entirely eliminate the risk of fraud or error.

# KEY PRINCIPLES OF EFFECTIVE INTERNAL CONTROL AND RISK MANAGEMENT

- Effective internal controls and risk management rely on several key principles.
  - Demonstrating commitment to integrity and ethical values
  - Establishing structure, authority, and responsibility
  - Ensuring accountability,
  - Effectively managing risk through assessment and mitigation.

# CONTROL ENVIRONMENT

- **Commitment to Integrity and Ethical Values:** Leaders must demonstrate a strong commitment to integrity/ethical behavior.
- **Board Oversight:** In order to ensure effectiveness of internal controls the board must exercise oversight responsibilities.
- **Structure, Authority, and Responsibility:** Effective internal control requires clear organizational structure, reporting lines, and defined responsibilities.
- **Competent Workforce:** To effectively manage risks and implement controls, organizations should attract, develop, and retain competent individuals.
- **Accountability:** Individuals must be accountable for their internal control responsibilities.



# CONTROL ENVIRONMENT

- **Commitment to Integrity and Ethical Values:** Leaders must demonstrate a strong commitment to integrity/ethical behavior.
- **Board Oversight:** In order to ensure effectiveness of internal controls the board must exercise oversight responsibilities.
- **Structure, Authority, and Responsibility:** Effective internal control requires clear organizational structure, reporting lines, and defined responsibilities.

## RISK ASSESSMENT

- **Competent Workforce:** To effectively manage risks and implement controls, organizations should attract, develop, and retain competent individuals.
- **Accountability:** Individuals must be accountable for their internal control responsibilities.
- **Objective Setting:** In order to properly identify and assess risks, clearly defined objectives are essential.

## RISK ASSESSMENT

- **Risk Identification and Analysis:** To properly execute the risk assessment process organizations must identify, analyze, and assess risks that could prevent them from achieving their objectives.
- **Fraud Risk:** COSO 2013 called special attention to the identification and assessing of fraud risks. This is management responsibility.
- **Significant Change Identification:** Changes in an organization operating environment and internal controls must be swiftly identified and analyzed with appropriate adjustments made to internal controls.

## CONTROL ACTIVITIES


- **Risk Mitigation:** Those risks identified during the risk assessment process should have appropriate developed control activities to mitigate risks in line with management risk tolerance
- **Technology Controls:** Technology controls are critical in today's digital age. Organizations must place a strategic focus on all controls over technology including general computer controls.
- **Policies and Procedures:** Controls should be based on thorough policies and procedures and these procedures should be properly communicated and trained on.

---

# BEST PRACTICES FOR IMPLEMENTING INTERNAL CONTROL IN FINANCIAL OPERATIONS

# INTERNAL CONTROL

- Internal control practices have existed since ancient times.
  - Hellenistic Egypt had a dual system of internal control in place for tax collecting: one set of bureaucrats collected the taxes while another oversaw that collection process.
- The term *internal control* was first defined in 1948 by the American Institute of Certified Public Accountants (AICPA).



**Internal Control**  
[in-'tər-nəl kən-'trōl]

The mechanisms, rules, and procedures implemented by a company to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud.

# INTERNAL CONTROL

- Several recent documents have defined and elaborated on internal control. They include:
  - The Integrated Internal Control Framework developed by the Committee of Sponsoring Organizations (COSO)
  - COBIT
  - ISO
- Internal controls assist organizations in presenting reliable financial reports to stakeholders, complying with laws and regulations, and having efficient and effective operations.

# INTERNAL CONTROLS

- To implement robust internal controls in financial operations, organizations should focus on establishing a strong control environment, assessing risks, designing and implementing control activities, providing information and communication, and monitoring controls.
- This involves a proactive approach to risk management, continuous improvement, and a commitment to ethical behavior and compliance.
- Many of the following principles tie directly to the COSO 2013 Internal Control Framework.



## ESTABLISH A STRONG CONTROL ENVIRONMENT

- **Ethical Culture:** In order to proliferate a strong control environment, management must promote a culture that values ethics, accountability, and compliance.
- **Clear Policies and Procedures:** As previously indicated, policies and procedures are key for implementing proper controls. The development and communication of detailed policies and procedures for financial transactions, expense reimbursements, and other high-risk areas is essential.
- **Employee Training:** It isn't good enough just to have the policies and procedures in writing,
  - The organization must provide adequate training to staff on their responsibilities and the importance of internal controls.

## ASSESS AND MANAGE RISKS

- **Risk Assessment:** Adequate, timely and appropriate risk assessment is critical to maintaining a strong organization and control environment.
  - Regularly assess and reassess risks, including both internal and external fraud risks, and potential errors in financial reporting.
- **Risk Mitigation:** When risks are identified during the risk assessment phase, they must be evaluated against management risk tolerance and then adequate controls must be developed and implemented controls to mitigate identified risks to a sufficient level.

## DESIGN AND IMPLEMENT EFFECTIVE CONTROL ACTIVITIES

- **Segregation of Duties:** Separate duties to prevent any single individual from having complete control over a transaction or process.
- **Authorization and Approval:** Implement proper authorization/approval processes for transactions and activities.
- **Reconciliations:** Regularly reconcile accounting records with external sources.

## DESIGN AND IMPLEMENT EFFECTIVE CONTROL ACTIVITIES

- **Physical Safeguards:** Secure physical assets and limit access to sensitive information.
- **Documentation and Record-Keeping:** Maintain accurate and detailed documentation of all financial transactions and activities.
- **Automation and Technology:** Utilize technology to automate processes, improve efficiency, and enhance control.

## INFORMATION AND COMPLIANCE

- **Clear Communication:** In the digital age, communication can move at lightening speed. It is essential that organizations ensure clear and effective communication of policies, procedures, and control responsibilities.
  - Personnel must understand their individual responsibility for internal control and how it links to their daily job tasks.
- **Reporting Mechanisms:** Establish channels for employees to report suspected fraud or other issues.
  - Hotlines, direct reporting methods, outsourced methods are all a possibility.

## MONITOR AND EVALUATE CONTROLS

- **Regular Internal Audits:** Although management should never just “wait till the auditors arrive” to become serious about internal controls, it is important to have a process to conduct regular internal audits to assess the effectiveness of controls.
- **Performance Reviews:** Performance reviews are often linked to personnel however organizations must also think of performance reviews as a time where they monitor control compliance and identify areas for improvement.
- **Control Testing:** Test controls to ensure they are operating effectively. This should be a process embedded into all areas and not one that waits till SOX compliance testing or auditor evaluation.

## KEY CONSIDERATIONS

- **Continuous Monitoring:** Continuously monitor controls and adapt them as needed to address changing risks.
- **Focus on Efficiency:** No one likes the bureaucracy that often comes with too many controls. It is important to implement controls efficiently and effectively, without creating unnecessary burden or disruption.

## KEY CONSIDERATIONS

- **Adapt to Change:** The world is ever evolving and the landscape of our business are changing. Regularly review and update controls to address changing business needs and regulations.
- **Technology and Automation:** Leverage technology to automate processes, improve efficiency, and enhance control.





# INTERNAL CONTROL FRAMEWORKS

25

25

Lynn Fountain  
Consulting and Training

# INTERNAL CONTROL FRAMEWORK

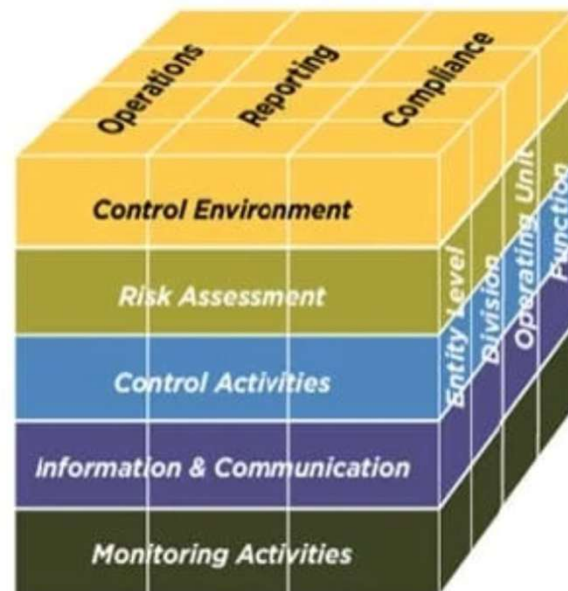
- An internal control framework is a structured guide that organizes and categorizes expected controls or control topics.
- Some organizations design control frameworks for general purposes like the COSO 2013 internal control framework, while others are more specific such as the COBIT IT Control framework.

# INTERNAL CONTROL FRAMEWORK

- When an organization uses a control framework effectively (typically in audit risk assessments and risk management), management designs internal control processes with the framework as a baseline.
- This helps the organization design control procedures that create and preserve value while minimizing risk.

## COSO 1992

- The topic of internal control cannot be discussed without reference to the COSO Integrated Internal Control Framework.
- It was developed in response to the need for effective ways to control enterprises.
- The framework provides principles-based guidance for designing/ implementing effective internal controls.



# COSO

- COSO established a committee that was a joint initiative of five private sector organizations (formed in 1985) to sponsor the National Commission on Fraudulent Financial:
  - 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)



# COSO

- The COSO Integrated Internal Control Framework formally defined *internal control* as “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with applicable laws and regulations
  - Safeguarding of assets

# COSO

- The framework defined five components of internal control. They include the following:
- **Control environment.** Sets the tone of an organization, influencing the control consciousness of its people. It is considered the “foundation” of internal control for an organization.
  - Exercise integrity and ethical values.
  - Make a commitment to competence.
  - Use the board of directors and audit committee.
  - Facilitate management’s philosophy and operating style.
  - Create organizational structure.
  - Issue assignment of authority and responsibility.
  - Utilize human resources policies and procedures.

# COSO

- **Risk assessment.** Provides for the identification and analysis of relevant risks to the achievement of objectives. It highlights that risk assessment should not be a “one and done.”
  - Risk assessment is an iterative process that occurs on a regular and ongoing basis. Included in this component is the concept of fraud risk analysis.
  - Create companywide objectives.
  - Incorporate process-level objectives.
  - Perform risk identification and analysis.
  - Manage change.



# COSO

- **Control activities.** Set of policies/procedures that ensure management directives are carried out.
  - They include concepts such as approvals, authorizations, verification controls, reconciliations, reviews of operating performance, security of assets, and segregation of duties, as well as relevant information technology controls.
    - Follow policies and procedures.
    - Improve security (application and network).
    - Conduct application change management.
    - Plan business continuity/backups.
    - Perform outsourcing.

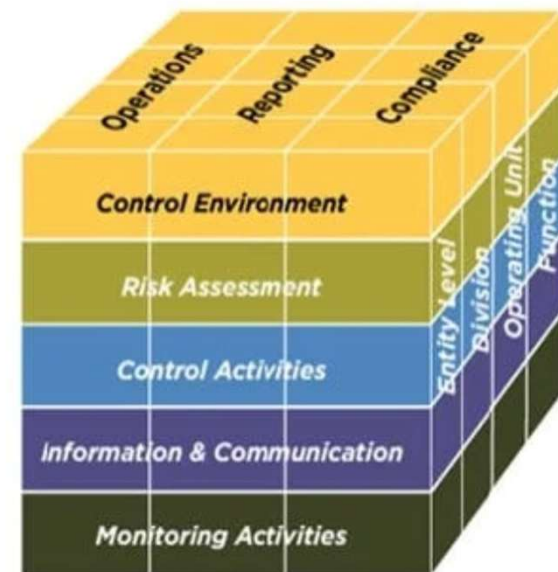
# COSO

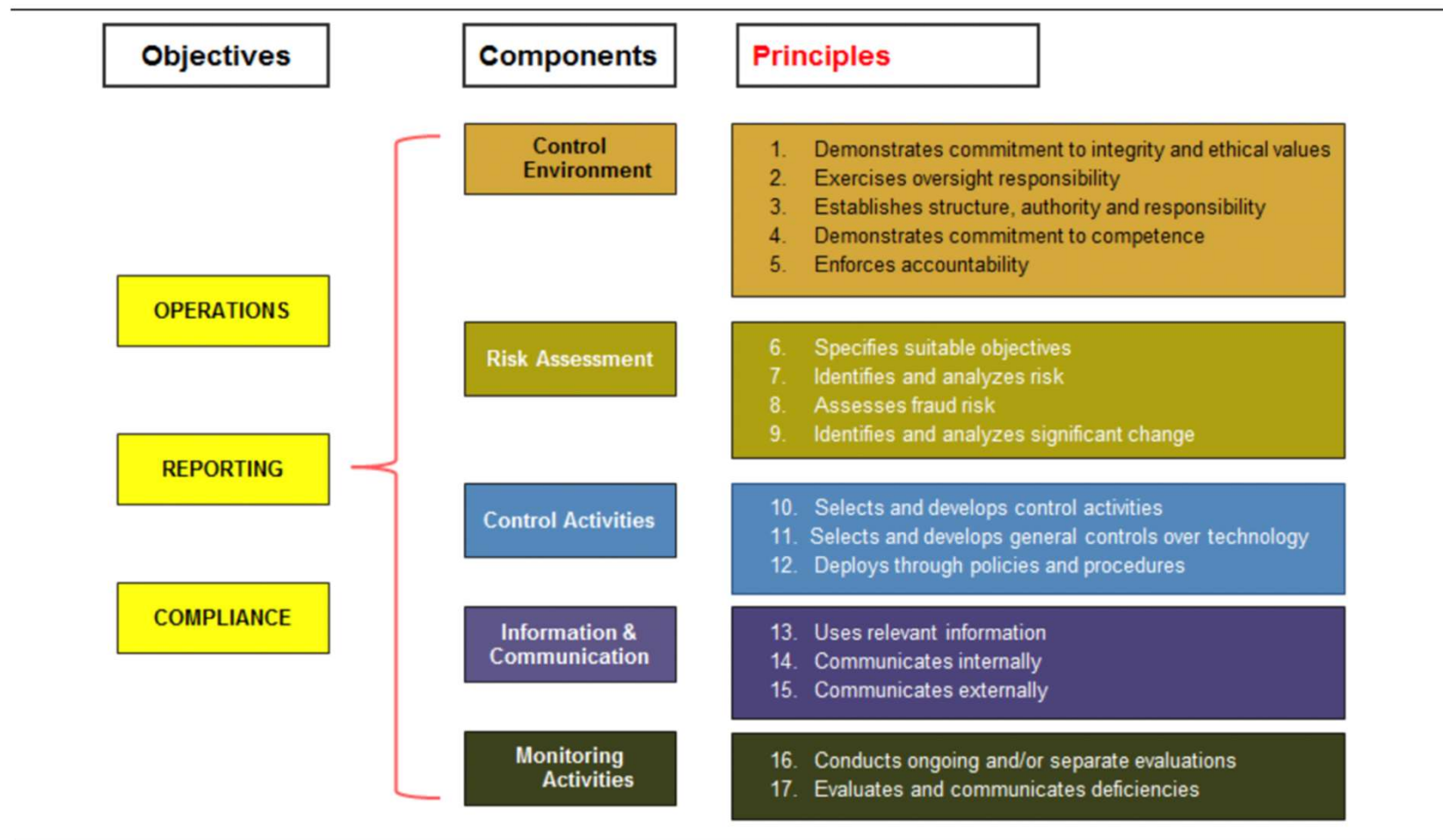
- **Information and communication.** Relates to the information technology systems that produce reports and make it possible to run and control the business.
  - It also relates to the methods utilized by the organization to communicate both internally and externally.
    - Measure quality of information.
    - Measure effectiveness of communication.

- **Monitoring.** Assesses the quality of the system's performance over time and is accomplished through ongoing activities or separate evaluations.
  - Perform ongoing monitoring.
  - Conduct separate evaluations.
  - Report deficiencies.

# COSO

- One of the primary changes to the framework is the formalization of 17 principles that underlie the five separate components of COSO.
- When developing the framework, COSO placed emphasis on ensuring it was scalable and suitable to all entities.







# COBIT

# COBIT

- Within the IT audit community, COBIT is the most popular IT control framework example.
- ISACA (Information Systems Audit and Control Association) owns the COBIT (Control Objectives for Information and Related Technology) framework and designed it for IT governance and management.
- It was created by ISACA to bridge the crucial gap between technical issues, business risks and control requirements.

# COBIT

- Some professionals refer to COBIT as a guideline aggregation framework.
- As an internal control integrated framework, it cross-references many of the other popular IT frameworks, making it an IT security framework that addresses the IT side of business risk.
  - **Purpose:** COBIT helps organizations ensure their IT investments/activities are aligned with business goals and contribute to achieving those objectives.



# COBIT

- **Scope:** COBIT covers a wide range of IT-related activities, including planning, organization, acquisition, implementation, delivery, and monitoring of IT resources.
- **Benefits:** By implementing COBIT, organizations can improve IT alignment with business objectives, enhance risk management, improve compliance, and ultimately achieve better business outcomes.

# PRINCIPLES AND DOMAINS OF COBIT

## ■ Principles

- Meeting stakeholder needs
- Covering the enterprise end-to-end,
- Applying a single integrated framework
- Enabling a holistic approach
- Separating governance from management

## ■ Domains

- Planning and Organization.
- Delivering and Support.
- Acquiring and implementation.
- Monitoring and Evaluation.

## COBIT VS COSO

- COSO and COBIT are both useful for creating, managing, maintaining internal controls.
  - COSO provides the overarching framework for fraud prevention through risk management
  - COBIT helps you to ensure that your IT system enhances and strengthens these controls.

## COSO VS. COBIT

- There's no single "better" framework between COSO and COBIT. Both frameworks serve distinct purposes.
  - COSO focuses on internal control and risk management across the entire organization,
  - COBIT is specifically tailored to IT governance and management.
  - The "best" choice depends on the organization's needs and objectives. Some organizations may leverage both frameworks to address different aspects of risk management and governance.

---

# ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION) FRAMEWORK

45

45

Lynn Fountain  
Consulting and Training

# ISO

- ISO standards, particularly ISO 27001 and ISO 19011, provide frameworks for internal controls, especially in the context of information security and audit programs.
  - ISO 27001 focuses on establishing an integrated internal control framework that aligns with industry best practices and addresses information security risks.
  - ISO 19011 provides guidelines for auditing management systems, ensuring audits are conducted consistently and effectively.
- **Purpose:** ISO 27001 is used to establish and maintain an information security management system (ISMS), which includes internal controls.
- **Approach:** Aligns with COSO, focusing on assessing/mitigating information security risks.

# ISO 27001 FRAMEWORK

- **Key Aspects:**
- Implementing policies, procedures, and organizational structures.
- Segregation of duties and authorization and approval processes.
- Performance monitoring and control procedures.
- Managing assets and resources.
- Conducting risk management and ensuring regulatory compliance.

# ISO 19001

- **Purpose:** ISO 19011 provides guidelines for auditing management systems. This assists organizations when implementing effective audit programs.
- **Benefits:**
  - Implementing auditing best practices.
  - Demonstrating credibility and capability in auditing.
  - Improving management systems and processes.
  - Meeting customer and regulatory audit requirements.
  - Facilitating consistent auditor training and evaluation.



## OTHER ISO STANDARDS

- **ISO 9001:** Often used for quality auditing. It can include internal controls related to quality management.
- **ISO 31000:** Provides guidance on risk management
- **ISO 45001:** Provides guidance on occupational health and safety management.
- In summary, ISO standards provide frameworks for internal controls in various contexts, including information security, auditing and risk management.

---

## STRATEGIES TO ENHANCE MONITORING, DOCUMENTATION, AND REPORTING OF CONTROLS.

50

50

Lynn Fountain  
Consulting and Training

# INTERNAL CONTROLS

- There are three main types of internal controls: detective, preventative, corrective.
  - Controls can be manual or automated.
  - Implementation of controls can be proactive (preventative) or reactive.
- Strongest assurance for internal controls is obtained from preventative and automated controls.



**Internal Control**  
*[in-'tər-nəl kən-'trōl]*

The mechanisms, rules, and procedures implemented by a company to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud.

 Investopedia

# INTERNAL CONTROLS

- **Detective Internal Controls** - Designed to find errors after they have occurred.
- Examples: cash counts, inventories, reviews and approvals, internal audits, peer reviews, or quality reviews and enforcement of job descriptions and expectations.
- Detective controls usually occur irregularly.



# INTERNAL CONTROLS

- **Preventative Internal Controls** - Put into place to keep errors/irregularities from happening.
  - Preventative controls usually occur on a regularly.
    - Examples: password transactions, testing for clerical accuracy, computer backup, drug testing, employee screening, segregation of duties, and approvals.



# INTERNAL CONTROLS

- **Corrective Internal Controls** -  
Correct errors found by the  
detective controls.
- Examples: reporting problems to a  
supervisor, training programs, and  
progressive discipline for errors.



---

# ARE INTERNAL CONTROLS INFALLIBLE?

55

55

Lynn Fountain  
Consulting and Training

# INTERNAL CONTROLS

- The mere fact that an internal control exists does not mean it will work properly.
- Controls can fail in many instances, including when:
  - They are not specified accurately or appropriately designed to meet the needs of the operation.
  - They do not function as specified or their failure to function is not detected.
  - They are deliberately circumvented.
  - Management views them as a blind utilization of forms, templates, and checklists.
  - There are too many mitigating controls.



# INTERNAL CONTROLS

- Just because an internal control procedure is working today doesn't mean it will continue to work in the future.
- Just because it has been working, that doesn't mean business changes haven't impacted its effectiveness.



# INTERNAL CONTROLS

- In some cases, professionals who focus on internal controls over financial reporting will correlate those controls to a particular financial statement assertion.
- There are five financial statement assertions in accounting.

## 5 Different Financial Statement Assertions

1. Existence.
2. Completeness.
3. Valuation.
4. Rights and Obligations.
5. Presentation and Disclosure.

## INTERNAL CONTROLS

- **Presentation and disclosure:** Accounts and disclosures are properly described in the financial statements of the organization.
- **Existence/occurrence/validity:** Only valid or authorized transactions are processed.
- **Rights and obligations:** Assets are the rights of the organization, and the liabilities are its obligations as of a given date.
- **Completeness:** All transactions are processed that should be.
- **Valuation:** Transactions are valued accurately using the proper methodology, such as a specified means of computation or formula.
- See Appendix for Clip Art on Assertions, Evidence and Audit Procedures

# INTERNAL CONTROLS

- Internal controls must be considered for all parts of the organization (not just the financial side).
- Following are common ways that auditors examine the assertions for financial statement review.
  - Use this opportunity to stretch beyond the financial statement impact of each of these assertions.
  - Think about how they may relate to operational or compliance processes.

# ASSERTIONS

- Transactions and events that occur in the organization
  - *Occurrence*: The transactions recorded have actually taken place.
  - *Completeness*: All transactions that should have been recorded have been recorded
  - *Accuracy*: The transactions were recorded at the appropriate amounts.
  - *Cutoff*: The transactions have been recorded in the correct accounting period.
  - *Classification*: The transactions have been recorded in the appropriate financial classification.

# ASSERTIONS

- Accounts balances as of period end:
  - *Existence*: Assets, liabilities, and equity balances exist and are reflective of the actual transactions of the organization.
  - *Rights and obligations*: The entity legally controls rights to its assets, and its liabilities faithfully represent its obligations.
  - *Completeness*: All balances that should have been recorded have been recorded.
  - *Valuation and allocation*: Balances that are included in the financial statements are appropriately valued, and allocation adjustments are appropriately recorded.

# ASSERTIONS

- Presentation and disclosure within the financial statements:
  - *Occurrence*: The transactions and disclosures have actually occurred.
  - *Rights and obligations*: The transactions and disclosures pertain to the entity.
  - *Completeness*: All disclosures have been included in the financial statements
  - *Classification*: Financial statements are clear and appropriately presented.
  - *Accuracy and valuation*: Information is disclosed at the appropriate amounts.

# ASSERTIONS

- The assertions that may most closely relate to operational transactions fall under the transactions and events that occur in the organization.
  - It is important that controls are in place to ensure a transaction (sale or services) has actually occurred, it is recorded completely and accurately and at the proper time, and it is properly classified.
- Let's use the following example and apply it to the sales process of a retail store.



## EXAMPLE

- Paul sells bedding at a large retail establishment. Paul's pay is based 100% on commission from his sales.
- Paul's friend (John) comes into the store, and Paul is his salesperson.

**EXAMPLE**

## EXAMPLE

- The organization should ensure it has the proper controls in place so that Paul does not take advantage of his relationship with his friend.
  - Collusion and scam sales or pricing kickbacks are a concern.
  - That means the organization should have procedures in place to ensure Paul properly writes up the customer order on a purchase order form, and that an independent individual verifies the pricing given to the customer.
- Also, Paul's supervisor should sign off on the transaction to ensure the materials ordered are appropriate and no unwarranted discounts are given.

## EXAMPLE

- John should submit the purchase order to his supervisor, who should validate the information and then forward it to the purchasing department.
  - These controls help ensure the transaction has actually occurred and is valid, complete, and accurate.
- As demonstrated by this example, internal controls must be applied to every facet of the organization to ensure propriety not only of financial controls but also of operational and compliance processes.



# STRATEGIES

## STRATEGIES

- To enhance monitoring, documentation, and reporting of controls, organizations should leverage technology, implement continuous monitoring systems, and ensure clear documentation processes.
- Automated tools can streamline testing and provide real-time insights, while centralized systems offer a unified platform for managing controls and reporting.

## TECHNOLOGY AND AUTOMATION

- **Automated Control Testing:** The ability to use automated tools will streamline control testing, reducing manual effort and increasing efficiency.
- **Continuous Monitoring Systems:** Implementing systems that provide real-time monitoring of control activities will allow for early detection of potential issues.
- **Data Analytics:** Utilizing data analytics to identify anomalies and patterns in control performance, enabling proactive remediation efforts.

## CENTRALIZED MANAGEMENT AND REPORTING

- **Centralized SOX Management Systems:** In today's world we have an abundance of centralized SOX management systems that can assist in managing SOX controls, tracking their status, and generating reports for regulatory compliance.
- **Audit Management Software:** This software has been in existence for many years but has advanced in its capabilities rapidly.
  - Utilize software to automate compliance monitoring, reporting, and documentation, reducing manual effort and ensuring consistency.

# DATA VISUALIZATION

- **Data Visualization:** This is a newer technique that is part of the digitization trend.
  - Employ data visualization tools to present control performance data in a clear and concise manner, enabling stakeholders to understand control effectiveness.
- **Documented Processes:** Maintain clear, up-to-date documentation of all control processes, including their design, implementation, and testing.
  - Remember, old procedures and documentation will cause great confusion to personnel trying to implement processes.



## SEGREGATION OF DUTIES

- **Segregation of Duties:** Clearly define, assign, and document segregation of duties within the internal control structure.
  - SOD is a key internal control principle where tasks are divided among different individuals to prevent fraud/errors. No single person should have complete control over a process or asset.
- **Regular Reviews:** Regularly review and update documentation to ensure accuracy and relevance.

# MONITORING

- **Regular Audits:** Conduct regular internal and external audits to assess control effectiveness and identify areas for improvement.
  - Even if you do not have an internal audit group, find a way to utilize a quality assessment process to evaluate areas.
- **Ongoing Monitoring Procedures:** Establish ongoing monitoring procedures to track control performance and identify potential deviations.
  - This is a true management responsibility.
- **Risk Assessments:** Conduct regular risk assessments to identify and prioritize financial risks, focusing control efforts where they are most needed.
  - Risk assessments are NOT just for the auditors.

## REPORTING

- **Reporting to Management and the Board:** Provide clear/concise reporting on control effectiveness to management and the board.
- **Data Analysis:** Analyze control performance data to identify trends and patterns, allowing for proactive remediation efforts.
- **Stakeholder Communication:** Communicate control performance data to relevant stakeholders



# RESPONSIBILITY FOR INTERNAL CONTROLS



# RESPONSIBILITY

- All individuals within an organization have some responsibility for internal control. Let's further evaluate how that may impact various categories of employees:
- *Employees* must fulfill their job description and understand the variance of job tasks versus internal controls. They must monitor their work to ensure proper execution and correction of errors in a prompt manner.
  - They must take reasonable steps to safeguard assets against waste, loss, and unauthorized use while adhering to organizational policies and procedures.

# RESPONSIBILITY

- *Managers* must ensure control procedures are operating effectively.
  - They must maintain a positive environment that encourages proper use of internal controls.
  - They must also develop, document, and monitor policies and procedures within their span of control.
  - To properly execute on this task, they must identify control objectives for their respective functions and implement cost- effective control strategies.
  - Managers are also responsible for testing controls to verify they are performing as intended.

# RESPONSIBILITY

- *The governing body* is tasked with the oversight of the proper functioning of internal controls.
  - Must apply due diligence and professional skepticism surrounding control processes.
  - Must challenge management on control processes and set a positive tone for adequate documentation of controls.
  - Must understand and enforce the COSO concepts.

## RESPONSIBILITY

- The most important aspect is the governing body understands the variance of control gaps vs control failures.
  - A control gap may indicate control procedures may not be sufficient to timely /readily identify an issue.
  - A control failure means that the control actually failed to perform for a specific process. In either case, both issues must be dealt with.





# INTERNAL CONTROL DOCUMENTATION

# DOCUMENTATION

- Documentation is the proof something exists or occurred.
  - It should support processes or conclusions of what was done.
- Documentation is critical to ensure strong control processes.



# DOCUMENTATION

- Control documentation may range from generic guidelines to detailed written policies, procedures, and flowcharts.
- Documentation can be critical for training, process improvement, and backup procedures; however, an excessive amount of documentation can also cause employee frustration and apathy.
- The trick is to find the proper balance for your organization.
- When beginning the task of documentation, think through the key elements of a transaction and identify those that should be documented.
  - The key elements to consider when determining what should be documented are process initiation, process authorization, process recording, and process reporting.

# DOCUMENTATION

- Consider the following questions:
  - Is there a potential for fraud to occur?
  - What if the person who performed the process is no longer available?
  - What if risks emerge that required a reevaluation of the entire process?
  - How can controls best be identified along with appropriate roles/ responsibilities?
  - What systems are used? Are the systems primary or secondary?
  - What is needed to support internal controls over financial reporting?
  - How does the process support the control objectives of completeness, accuracy, validity, and restricted access?
  - What would be needed to re-create the process in the event of business interruption?
  - What management responsibilities should be documented?

# DOCUMENTATION

- In essence, determine which controls are necessary to the process, activity, or system under review in light of the risk profile and desired level of control.
  - Your goal is to be able to document how the transaction was initiated, authorized, recorded, and reported. Choice of documentation methods is up to management and process owners.
  - Use what works for your organization.

# DOCUMENTATION

- **Flowcharts.** Used to describe the flow of activity through a process, as well as the relevant documentation.
  - The output is a process map, which is a graphical representation of events performed by a group of people.
- **Narratives.** Narratives describe process flows in written form, without graphical representations.
  - A useful supplement to flowcharts by detailing existing practices.
  - Independently, narrative descriptions are not an effective tool for process description.
    - Critical because they can often exclude critical information on control points.

# DOCUMENTATION

- **Policies and procedures.** These are manuals that establish a systematic framework and guidelines for an organization's processes.
- They facilitate implementation of business strategy on both a strategic and an operational level.

## Policies

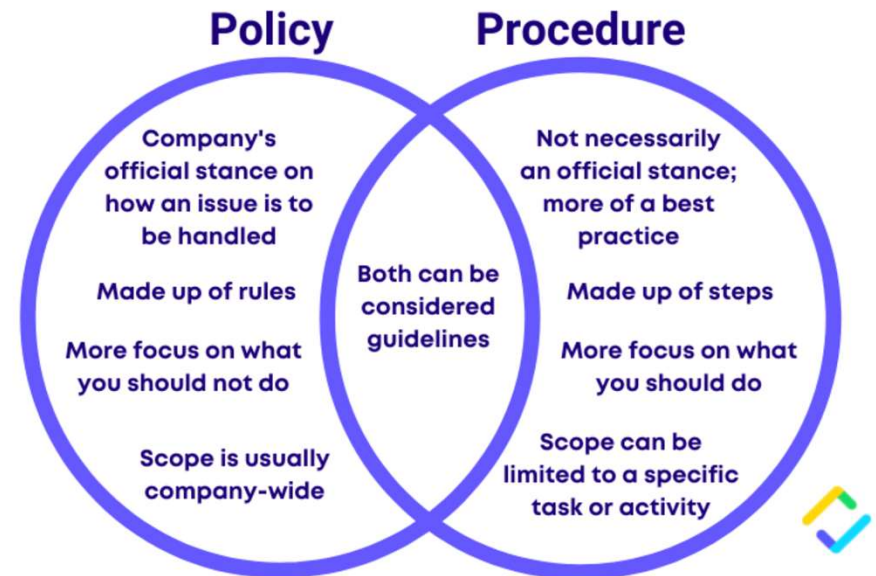
- Are general in nature
- Identify company rules
- Explain why they exist
- Tells when the rule applies
- Describe who it covers
- Shows how the rule is enforced
- Describes the consequences
- Are normally described using simple sentences and paragraphs

## Procedures

- Identify specific actions
- Explain when to take actions
- Describe alternatives
- Shows emergency procedures
- Includes warning and cautions
- Gives examples
- Shows how to complete forms
- Are normally written using and outline format

# POLICY VS PROCEDURE: WHAT IS THE DIFFERENCE?

- The difference between policy and procedure is that policy requires organizations to take a stand or make a decision on how to approach a specific problem occurring in the workplace.
- A procedure requires organizations to agree on how to perform a task for the best results.





# DOCUMENTATION

- **Questionnaires.** Should be designed to assist in the identification and evaluation of internal controls.
  - Documents must be carefully structured and logically sequenced with a series of questions that assist in the documentation of processes.
  - Focus should be placed on areas where control gaps may exist along with control strengths and weaknesses.

## DOCUMENTATION

- **Risk and control matrices.** These are spreadsheet-type documents that allow for linkage of controls with control objectives and related risks.
  - Designed both to document risks/controls and to facilitate evaluation of the design and effectiveness of the control system.
  - Regularly used for internal control over financial reporting.

# HOW AND WHAT TO DOCUMENT

- Regardless of the method you utilize to document controls, the following suggestions will assist you in creating solid process documentation that will enhance your level of internal control.
  - Identify the initial inputs to the process. - Every transaction originates from a source.
  - Identify the point of initiation, including documents utilized in the process.

# DOCUMENTATION

- Depict each successive step in the process (manual and automated) in a logical sequence.
  - The description should be short and concise but detailed enough for a reader to understand the event.
  - Describe key events, actions, or decisions as they occur until transactions are recorded and the process is concluded.
- Identify controls related to information technology (IT).
  - Identify the relevant IT controls within the documentation and describe the risks related to relevant IT controls.

# DOCUMENTATION

- Identify key outputs of the process.
  - Understand how data is entered and processed within the IT system as well as the flow of data from initiation to recording of the transaction. Show the final disposition of all transactions.
- Identify points in the process where controls exist and where there are potential control gaps.
- Proper documentation of internal controls will facilitate an effective, efficient process that can be replicated and managed to ensure internal controls are appropriately managed.



# SUMMARY

94

## SUMMARY

- This course has focused on the many concept of internal controls.
  - Remember, internal controls are everyone's responsibility.
- We discussed the COSO Integrated Internal Control Framework and what it means for internal control.
- We reviewed methods to identify and document internal controls
- See written narrative appendix for a generalized checklist of internal controls for various processes.



# APPENDIX



# Assertions, Evidence and Audit Procedures

PCAOB Assertions	ASB Assertions	Key Questions	Examples of Evidence Available	Representative Audit Procedures
Existence or occurrence	Existence	Do the assets recorded really exist?	The physical presence of the assets	Inspection of tangible assets
	Occurrence	Did the recorded sales transactions really occur?	Client shipping documents	Inspection of records or documents (vouching)
Completeness	Completeness	Are the financial statements (including footnotes) complete?	Documents prepared by the client	Inspection of records or documents (tracing)
	Cutoff	Were all transactions recorded in the proper period?	Client receiving, shipping reports	Inspection of records or documents (tracing or vouching)
Rights and obligations	Rights and obligations	Does the entity really own the assets? Are related legal responsibilities identified?	Statements by independent parties	Confirmation
Valuation and allocation	Valuation or allocation	Are the accounts valued correctly?	Client-prepared accounts receivable aging schedule	Reperformance
	Accuracy	Were transactions recorded accurately?	Vendor invoices	Inspection of records or documents (tracing or vouching)
Presentation and disclosure	Classification	Were all transactions recorded in the proper accounts?	Comparisons of current-year amounts with those from the prior year	Analytical procedures
	Understandability	Are the presentations and disclosures understandable to users?	Management-prepared financial statements and footnotes	Inquiry