INFO AUDITING 6008

WEEK 1 - COSO

FANSHAWE

History of Auditing

- The profession of auditing has been with us for a long time. Mesopotamian scribes in around 3000 BC utilized elaborate systems of internal controls using stone documents that contained ticks, dots, and checkmarks.
- Historically, auditing was concerned with accounting for government activities and reviewing the work done by tax collectors.
- In the early years of auditing, the keeping and maintaining of accounting records was done primarily to detect fraudulent activity.

History of Auditing

- The industrial revolution in the mid 1700s to the mid 1800s was responsible for the increased demand in auditors.
- As such this period saw an increase in responsibility being passed from owners to managers.
- This led to an increased requirement for auditors who were independent of management and who were engaged not only to be alert for errors within financial records but also errors within the records.
-

History of Auditing

- In simple terms, deliberate errors in order to achieve personal financial gain were deemed to be fraudulent activity (as is still the case today) whilst error was (and still is) unintentional.
- During the early 1700s the concept of ‘sampling’ was introduced. Sampling is where auditors select a sample of items that make up various balances and was used where it is not economically viable to physically examine all the transactions that have taken place.
- The practice of sampling is still pivotal today.

Defining Auditing

- Most internal auditors follow high-level standards established by the Institute of Internal Auditors (IIA; www.theiia.org), but there are many different practices and approaches to internal auditing today due to its worldwide nature and wide range of auditing activities.
- An effective way to begin understanding internal auditing and its key areas is to refer to the internationally recognized internal audit professional organization, the IIA, and its published professional standards that define the practice:

Defining Auditing

“Internal auditing is an independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization”.

- *Independent* is used for auditing that is free of restrictions that could significantly limit the scope and effectiveness of any internal auditor review or the later reporting of resultant findings and conclusions.

Defining Auditing

- *Appraisal* confirms the need for an evaluation that is the thrust of internal auditors as they develop their conclusions.
- *Established* confirms that internal audit is a formal, definitive function in the modern enterprise.

Defining Auditing

- *Examine and evaluate* describe the active roles of internal auditors, first for fact-finding inquiries and then for judgmental evaluations.
- *Its activities* confirm the broad jurisdictional scope of internal audit work that applies to all of the processes and activities of the modern enterprise.

External and Internal Audits

- External and Internal IT audits share a common focus: the internal controls implemented and maintained by the organization being audited.
- Controls are a central element of IT management, defined and referenced through:

standards, guidance, methodologies, and frameworks

Addressing business processes; service delivery and management; information systems design, implementation, and operation; information security; and IT governance.

External and Internal Audits

- Leading sources of IT governance and IT auditing guidance distinguish between *internal control* and *internal controls*.
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines *internal control* as a process “designed to provide reasonable assurance regarding the achievement of objectives” including operational effectiveness and efficiency, reliable reporting, and legal and regulatory compliance.
- In this context, a *control* is “a policy or procedure that is part of internal control,” the result of policies and procedures designed to effect control.

The COSO Framework

- Who or what is *COSO*?
- COSO is a framework.
- COSO *internal controls* is a framework outlining professional practices for establishing preferred business systems and processes that promote efficient and effective internal controls.

The COSO Framework

- Whether operating in an industry environment, as an IT specialist internal auditor, or in not-for-profit or governmental sectors, every internal auditor should possess an understanding of the COSO internal control framework.

The COSO Framework

- In the early part of this century, a series of major accounting frauds and business failures in the United States and elsewhere became a call for external auditing and corporate governance reforms.
- The result was the Sarbanes-Oxley Act (SOx) in the United States

The COSO Framework

- Although the SOx legislation is very broad and has regulations and rules, a knowledge and understanding of the SOx internal control review procedures is a requirement for all internal auditors working at least with public corporations.
- In addition, all internal auditors should have general understanding of the SOx internal control and its corporate governance rules.

The COSO Framework

- The fundamental provisions of SOx can be divided into the five categories of corporate governance:

1) financial reporting,
2) audit functions,
3) federal securities
4) law enforcement, and
5) others (e.g., legal counsel, financial analysts).

The COSO Framework

- The provisions of the act that were not previously practiced by public companies and that are intended to benefit all companies are the following:
- Creating the Public Company Accounting Oversight Board (PCAOB) https://pcaobus.org to regulate and oversee the audit of public companies and to improve the ineffective self-regulatory environment of the auditing profession.

The COSO Framework

- Improving corporate governance through more independent and vigilant boards of directors, particularly effective and mandatory audit committees for public companies.
- Enhancing responsibilities of executives of public companies by requiring certification of financial statements by both the chief executive officer (CEO) and the chief financial officer (CFO).

The COSO Framework

- Enhancing the quality, reliability, transparency, and timeliness of financial disclosures through executive certifications of both financial statements and internal controls.
- Regulating the conduct of auditors, legal counsel, and financial analysts, and their potential conflicts of interest, increasing civil and criminal penalties for violations of security laws, and rebuilding public trust and investor confidence in public financial reports and financial markets.

COSO Internal Controls

- COSO *internal controls* is a framework.
- It outlines professional practices for establishing preferred business systems and processes that promote efficient and effective internal controls.
- The sponsoring organizations that issue and publish this material are neither governmental nor some other type of regulatory agencies.

COSO Internal Controls

- The *COSO internal control framework* is an important set or model of guidance materials that enterprises should follow when developing their business processes, systems, and procedures as well as in establishing *Sarbanes-Oxley Act (SOx)* compliance.

COSO Internal Controls

- The *COSO internal control framework* is an important set or model of guidance materials that enterprises should follow when developing their business processes, systems, and procedures as well as in establishing *Sarbanes-Oxley Act (SOx)* compliance.

COSO Internal Controls

- The COSO internal control framework was originally launched in the United States in 1992.
- This 1992 COSO internal control framework became a fundamental element of the American Institute of Certified Public Accountants (AICPA) auditing standards in the United States

COSO Internal Controls

- This 1992 COSO internal control framework eventually became the standard for enterprise external auditors in their reviews certifying that *enterprise internal controls* were adequate following the SOx
- Because of its general nature describing good internal control practices, the COSO framework had never been revised until 2014.

COSO Internal Controls

- Since the release of that original COSO framework, there have been many changes in business organizations and particularly in enterprise structures and IT processes.
- For example, mainframe computer systems with lots of batch processing procedures were common then but have all but gone away today, to be replaced by client-server and wireless systems.
- Because of the Internet, enterprise organizational structures have become much more fluid, flexible, and international.
- Things like social network computing, powerful handheld devices, and cloud computing did not exist back then.

COSO Internal Controls

- The original COSO internal control framework, released in 1992, provided an excellent description of this multidimensional concept, defining internal control as follows:
- Internal control is 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:

COSO Internal Controls

- Effectiveness and efficiency of operations
- Reliability of *financial reporting*
- Compliance with applicable laws and regulations
- COSO originally used a three-dimensional model to describe an internal control system in an enterprise.

COSO Internal Controls

- The revised COSO Framework (2013) replaces the 1992 and 2006 Framework guidance and documents. Those prior publications will be considered superseded after December 15, 2014.

COSO Internal Controls

- Some key elements of the new guidance include retention of the five basic components:

1. control environment
2. risk assessment
3. control activities
4. information and communication
5. monitoring

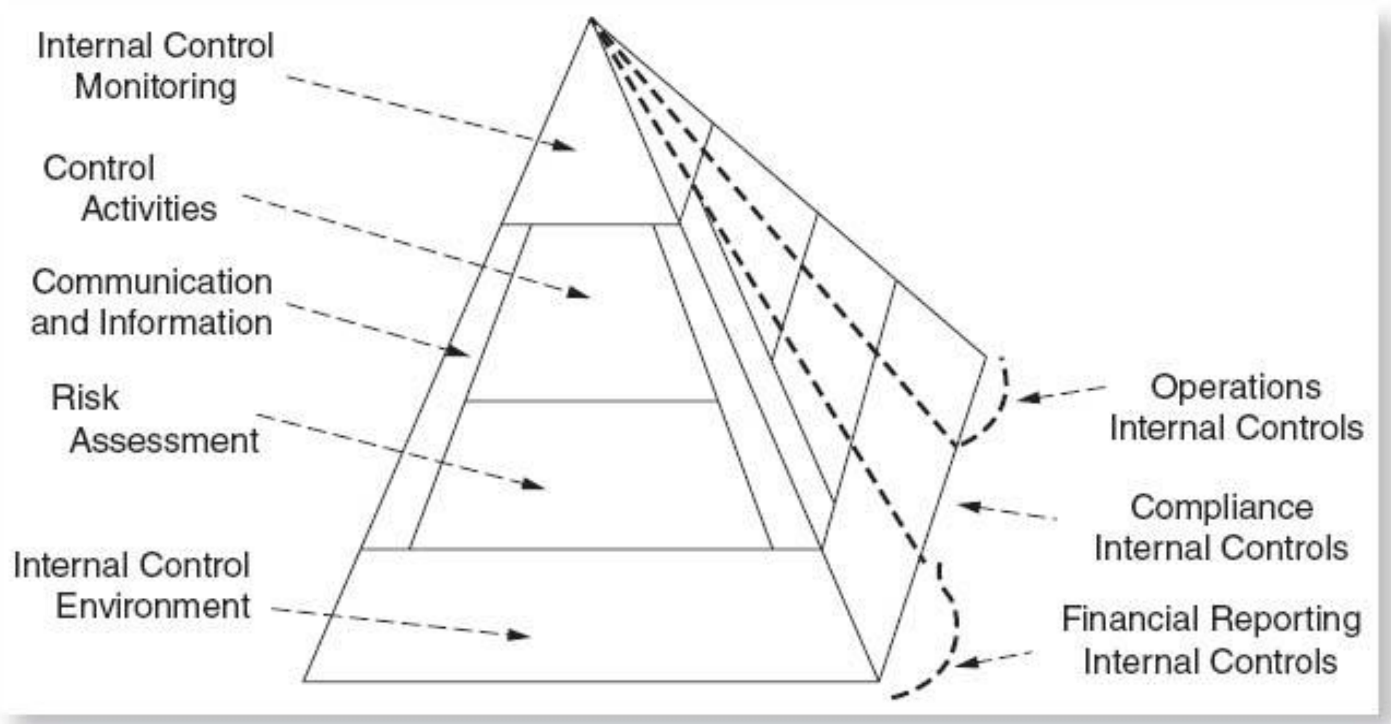
COSO Internal Controls

- Identification of 17 Principles that are deemed essential to the five components.
- Clear expectations that the elements of internal control work together in an integrated way.

COSO Internal Controls

- COSO **originally** used a three-dimensional model to describe an internal control system in an enterprise.
- The ensuing diagram illustrates the original COSO model of internal control as a pyramid with five layers or interconnected components comprising the overall internal control system.

COSO Internal Controls


Internal Control Monitoring
Control Activities
Communication and Information
Risk Assessment
Internal Control Environment
Operations Internal Controls
Compliance Internal Controls
Financial Reporting Internal Controls

COSO Internal Controls

- The COSO model was quickly adopted by the auditing and accounting profession, first in the US and then worldwide.
- It became significant after the Sarbanes-Oxley Act (SOx) became law.
- SOx requires that public reporting organizations must attest to the adequacy of their internal controls, using the COSO framework as a measure.

COSO Internal Controls

- While the basic concepts of internal controls have not much changed since that original COSO framework, the overall environment where business operates and internal auditors perform their reviews has changed a lot, including some of the following:

COSO Internal Controls

- **The rise of using contracted services, new organizational structures, and increased international connections.**

While the single monolithic corporation, such as Ford Motor of some 100 years ago, is largely a thing of the past, organizational relationships today are often increasingly complex, with the use of contracted services, joint ventures, and different international business arrangements.

COSO Internal Controls

- **Increased compliance and regulatory requirements beyond just annual financial reporting.**

Enterprises today are faced with multiple requirements to build and manage systems that are in compliance with a vast range of standards and legal and regulatory requirements, both in their own country and internationally.

COSO Internal Controls

Recognition that fraud prevention and detection is necessary for effective internal controls.

- In years past, *fraud detection* and prevention measures were not considered to be accounting and auditing concerns but legal and enterprise security issues.
- These matters were still not part of the original COSO framework, but attitudes have totally changed in recent years and internal auditors now have major responsibilities for fraud-related issues.

COSO Internal Controls

Increased needs for understanding and assessing risk as part of internal control operations on all levels.

- Understanding and managing risk has become an increased requirement for internal auditors since the original COSO framework.
- While that original framework highlighted understanding risks as an internal control component, our understanding and concerns here have grown dramatically.

COSO Internal Controls

The constant changes in IT technologies and the way we use IT to build and manage processes.

- If there is any area that has changed the most since the original COSO framework, it is the growth and prevalence of IT-related processes and technologies.

COSO Internal Controls

Ever-increasing security concerns, particularly IT security in today's big data era.

- At the time of the original COSO framework, enterprise security concerns in general were far less of an issue and IT security often represented little more than a secure lock on the mainframe computer center door.
- How things have changed! A mixture of various Internet-based threats and general terrorism concerns worldwide have expanded internal control concerns.

COSO Internal Controls

- **Internal control implications associated with social media and wireless systems.**
- This is a totally new and evolving area since the original COSO framework was released.
- Social media systems such as Facebook now allow enterprise associates and others to get around enterprise rules and also to communicate with handheld wireless devices.

Revised COSO Internal Controls

- Recap that COSO, or the Committee of Sponsoring Organizations of the *Treadway Commission*, is a joint initiative of five private-sector professional accounting, auditing, and finance organizations.
- COSO is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence.
- The new COSO internal control framework and its supporting guidance materials contain changes in the following areas:

Revised COSO Internal Controls

Expanded expectations for governance oversight.

- Increasing regulatory requirements and stakeholder expectations require boards of directors to increase their emphasis on the adequacy of internal financial controls in their enterprises.

Increased globalization of markets and operations.

- Enterprises today increasingly expand beyond their traditional domestic markets in pursuit of value, often entering into international markets and engaging in cross-border mergers and acquisitions.

Revised COSO Internal Controls

Changes and greater complexities in enterprise business operations.

- Enterprises change their business models and enter into complex transactions in the pursuit of growth, greater quality, or productivity, as well as in response to changes in markets or regulatory environments. These changes may involve entering into joint ventures, strategic alliances, or other complex arrangements with external parties, implementing shared services, and engaging with outsourced service providers.

Revised COSO Internal Controls

Increased demands and complexities in laws, rules, regulations, and standards.

- Governmental authorities are increasingly releasing complex rules and legislation where compliance is often difficult to achieve and where these rules do not directly follow classic internal control approaches.

Revised COSO Internal Controls

Ever-increasing use of and reliance on evolving technologies.

- As we have highlighted in our introduction to this chapter, the growth of IT systems and related technologies has very much changed our approaches to implementing and managing internal control processes. Today’s IT systems are increasingly based on automated internal controls and processes to build, install, and monitor these automated controls.

Revised COSO Internal Controls

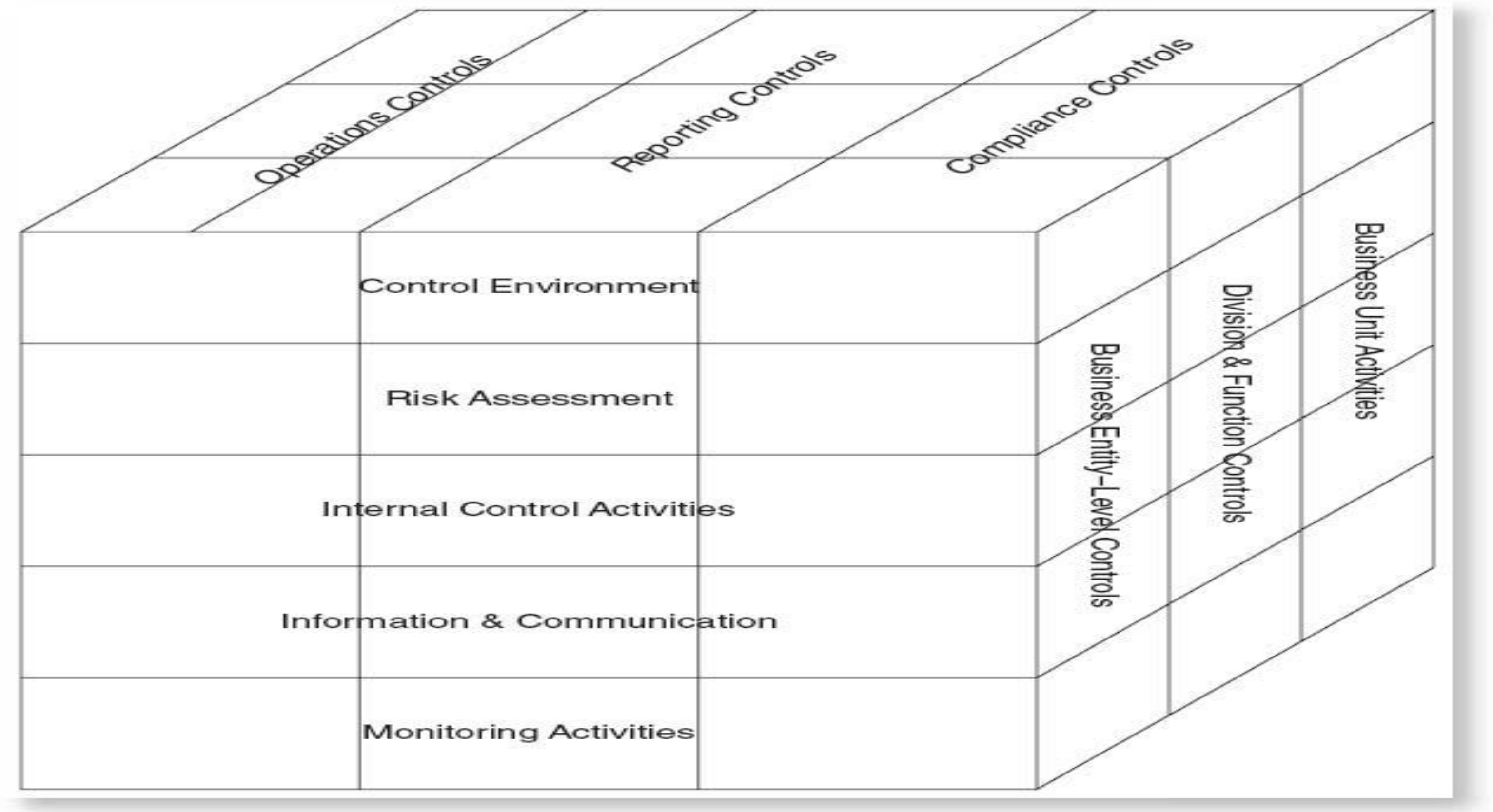
Increased need to prevent and detect corruption.

- The U.S. *Foreign Corrupt Practices Act*, introduced many years ago was an earlier example of legislation to increase internal control and other legal requirements. Today, there is a wide range of anticorruption and antifraud rules and legislation in place, including international as well as often differing rules in many U.S. states.

Revised COSO Internal Controls

- In addition to the three internal control objective categories of operations, reporting, and compliance the COSO framework defines internal controls from two other dimensions or perspectives: separate components of internal control and organization factors.
- The following diagram shows the revised three-dimensional COSO internal control framework.

Revised COSO Internal Controls



Revised COSO Internal Controls

- The three categories of *internal control objectives*

1. operations
2. reporting,
3. compliance

are represented by the columns defined at the top of the diagram.

Revised COSO Internal Controls

- The front-facing side of this COSO cube diagram defines five key components or levels of internal control:

1. Control environment
2. *Risk assessment*
3. Internal control activities
4. Information and communication
5. Monitoring activities

Revised COSO Internal Controls

- On the right-facing side of the model, is the third important dimension of internal control. It represents the internal control–related components of the overall organization structure:
- the enterprise entity itself,
- its divisions, subsidiaries,
- operating units, or functions, including business processes such as sales, purchasing, production, and marketing.

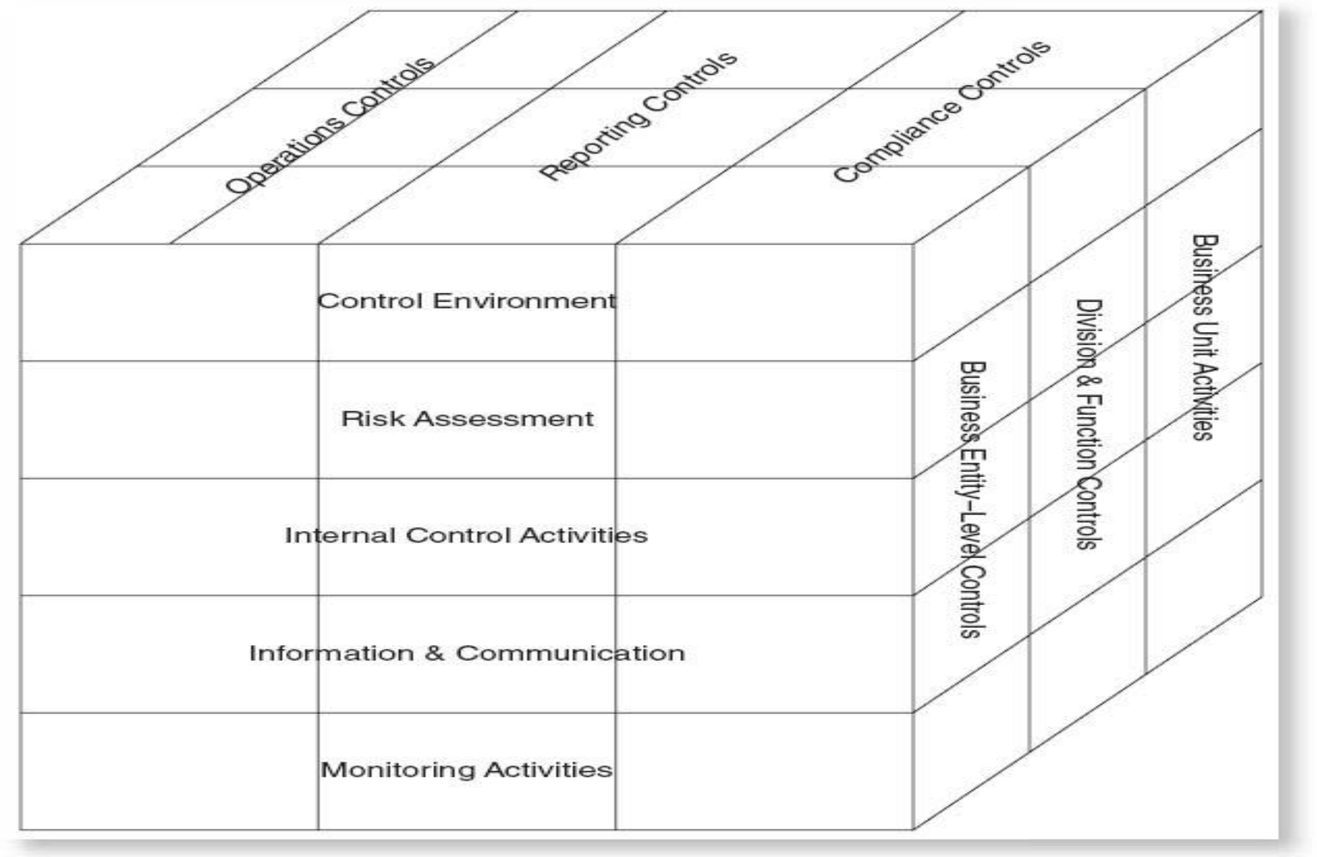
Revised COSO Internal Controls

- As an example, assume an EU–based enterprise has launched a new business product sales venture in Myanmar (Burma), a country that had been closed to the outside world until recently.
- With limited IT resources and telecommunication connections, we can expect different control processes in the Myanmar facility than would be found in the entity's headquarters operations.
- So additional processes such as the use of supporting manual control procedures should be established to achieve internal controls at the overall entity level.

COSO Internal Control Principles

- The revised COSO framework now codifies a set of principles that support the five components of internal control.
- The revised version explicitly defines 17 internal control principles representing fundamental concepts associated with the 5 components of internal control.
- COSO makes these principles explicit to increase management’s understanding as to what constitutes effective internal control.

Revised COSO Internal Controls



Element	Principle
Control environment	1. Demonstrate commitment to integrity and ethical values 2. Ensure that board exercises oversight responsibility 3. Establish structures, reporting lines, authorities, and responsibilities 4. Demonstrate commitment to a competent workforce 5. Hold people accountable
Risk assessment	6. Specify appropriate objectives 7. Identify and analyze risks 8. Evaluate fraud risks 9. Identify and analyze changes that could significantly affect internal controls
Control activities	10. Select and develop control activities that mitigate risks 11. Select and develop technology controls 12. Deploy control activities through policies and procedures
Information and communication	13. Use relevant, quality information to support the internal control function 14. Communicate internal control information internally 15. Communicate internal control information externally
Monitoring	16. Perform ongoing or periodic evaluations of internal controls (or a combination of the two) 17. Communicate internal control deficiencies

COSO - The Control Environment

- The set of standards, processes, and structures that provide a basis or structure for carrying out effective internal control activities across an enterprise.
- The control environment includes the actions of the board of directors and senior management who take responsibility for overall internal controls and expected standards of conduct.

COSO - The Control Environment

- The control environment comprises:
- integrity and ethical values of the enterprise;
- parameters enabling the board of directors to carry out its oversight responsibilities;
- organizational structure and assignment of authority and responsibility;
- processe57s for attracting, developing, and retaining competent individuals;
- rigor around performance measures, incentives, and rewards to drive accountability for performance.

COSO - The Control Environment

- An effective control environment creates the discipline that supports the assessment of risks necessary for the achievement of the entity’s objectives, performance of control activities, use of information and communication systems, and conduct of monitoring activities.

COSO - The Control Environment

- The COSO control framework introduces four internal control environment principles as:

COSO - The Control Environment

1. An enterprise should specify objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
2. The enterprise should identify risks to the achievement of its objectives across the entity and analyze risks as a basis for determining how they should be managed.
3. The organization should consider the potential for fraud in assessing risks to the achievement of objectives.
4. The organization should identify and assess changes that could significantly impact the system of internal control.

COSO - The Control Environment

An enterprise’s control environment is also synonymous with its internal control culture. Elements of a strong culture, such as integrity and ethical values, oversight, accountability, and performance evaluations, make the control environment strong as well.

Culture is part of an enterprise’s control environment, but also encompasses elements of other components of internal control, such as establishing effective policies and procedures, ease of security controls or access to information, and responsiveness to the results of monitoring activities.

COSO - The Control Environment – Look at the tree!

- Enterprises are led from the top by senior management and the board of directors, and their business ethics and philosophies will be passed down to all levels of employees and stakeholders.
- The more ethical and responsible the management style, the more likely that employees will respond to that style and behave in an ethical and responsible manner. Alternately, if management shows little concern for honest and ethical behavior, the employees will follow that lead.

COSO Internal Control Components: Risk Assessment

- Risk assessment is a key element in the COSO internal control framework. Risks are defined here as the possibility that an event may occur that will adversely affect the achievement of enterprise objectives.
- The management of internal control risks affects an enterprise’s ability to succeed, compete within its industry, maintain its financial strength and positive reputation, and maintain the overall quality of its products, services, and people.

COSO Internal Control Components: Risk Assessment

- The COSO internal guidance materials outline a series of risk assessment principles with the following four key concepts:

1. The enterprise should specify objectives with sufficient clarity to enable the identification and assessment of risks relating to those objectives.
2. The enterprise should identify risks to the achievement of its objectives across the entity and should analyze risks as a basis for determining how those risks should be managed.
3. The enterprise should consider the potential for fraud in assessing risks to the achievement of objectives.
4. The enterprise should identify and assess changes that could significantly impact its system of internal controls.

COSO Internal Control Components: Risk Assessment

- Enterprise management at all levels should endeavor to identify all possible risks that may impact the success of the enterprise, ranging from the larger or more significant risks to the overall business down to the less major risks associated with individual projects or smaller business units.
- The risk identification process should occur at multiple levels in an enterprise. A risk that impacts an individual business unit or project may not have that great of an impact on the entire enterprise, but a major risk that impacts the entire economy will flow down to the individual enterprise and the separate business units.

COSO Internal Control Components: Risk Assessment

- Identifying and analyzing risks should be an ongoing iterative process conducted to enhance an enterprise’s ability to achieve its objectives. Internal audit can often play a powerful role here as it builds and establishes what is often called an audit universe.

COSO Internal Control Components: Risk Assessment

- Types of Enterprise Business Risks:

Strategic Risks		
External Factors Risks	Internal Factors Risks	
▪ Industry Risk ▪ Economy Risk ▪ Competitor Risk ▪ Legal and Regulatory Change Risk ▪ Customer Needs and Wants Risk	▪ Reputation Risk ▪ Strategic Focus Risk ▪ Parent Company Support Risk ▪ Patent/Trademark Protection Risk	

COSO Internal Control Components: Risk Assessment

Operations Risks		
Process Risks	Compliance Risks	People Risks
▪ **Supply Chain Risk** ▪ **Customer Satisfaction Risk** ▪ **Cycle Time Risk** ▪ **Process Execution Risk**	▪ Environmental Risk ▪ Regulatory Risk ▪ Policy and Procedures Risk ▪ Litigation Risk	▪ Human Resources Risk ▪ Employee Turnover Risk ▪ Performance Incentive Risk ▪ Training Risk

COSO Internal Control Components: Risk Assessment

Finance Risks		
Treasury Risks	Credit Risks	Trading Risks
▪ **Interest Rate Risk** ▪ **Foreign Exchange Risk** ▪ **Capital Availability Risk**	▪ Capacity Risk ▪ Collateral Risk ▪ Concentration Risk ▪ Default Risk ▪ Settlement Risk	▪ Commodity Price Risk ▪ Duration Risk ▪ Measurement Risk

COSO Internal Control Components: Risk Assessment

Information Risks

Financial Risks	Operational Risks	Technology Risks
▪ **Accounting Standards Risk** ▪ **Budgeting Risk** ▪ **Financial Reporting Risk** ▪ **Taxation Risk** ▪ **Regulatory Reporting Risk**	▪ Pricing Risk ▪ Performance Measurement Risk ▪ Employee Safety Risk	▪ Information Access Risk ▪ Business Continuity Risk ▪ Availability Risk ▪ Infrastructure Risk

COSO Internal Control Components:
RISK RESPONSE STRATEGIES

As part of establishing effective COSO internal controls, enterprises should also develop risk management strategies to address how they intend to assess, respond, and monitor risk.

COSO internal control guidance materials identify four basic risk response strategies approaches:

COSO Internal Control Components:
RISK RESPONSE STRATEGIES

1. Avoidance
2. Reduction
3. Sharing
4. Acceptance

COSO Internal Control Components:

RISK RESPONSE STRATEGIES

- **Avoidance.** This is a strategy of walking away from the risk—such as selling a business unit that gives rise to the risk, exiting from a geographical area of concern, or dropping a product line.
- The difficulty here is that enterprises often do not drop a product line or walk away until after the risk event has occurred with its associated costs.
- Avoidance can be a potentially costly strategy.

COSO Internal Control Components:
RISK RESPONSE STRATEGIES

- **Reduction.** A wide range of business decisions may be able to reduce certain risks. Product line diversification may reduce the risk of too strong a reliance on one key product line.
- Splitting an IT operations center into two geographically separate locations may reduce the risk of some catastrophic failure.
- There are a wide range of often effective strategies to reduce risks at all levels that go down to the mundane but operationally important step of cross-training employees.

COSO Internal Control Components:
RISK RESPONSE STRATEGIES

- **Sharing.** Virtually all enterprises as well as individuals regularly hedge or share some of their risks by purchasing insurance. Many other techniques are available here as well.
- For financial transactions, an enterprise can engage in hedging operations to protect from possible price fluctuations.
- The idea is to arrange to have another party accept some of a potential risk, with the recognition that there will be costs associated with that activity.

COSO Internal Control Components:
RISK RESPONSE STRATEGIES

- **Acceptance.** This is the strategy of no action. An enterprise can "self-insure" itself rather than purchase an insurance policy.
- Essentially, an enterprise should look at a risk's likelihood and impact in light of its established risk tolerance and then decide whether or not to accept that risk.
- For the many and varied risks that approach an enterprise, acceptance is often the appropriate strategy for some risks.

COSO Internal Control Components: Internal Control Activities

- Perhaps the core element in the overall COSO internal control framework, control activities are the actions—established through enterprise policies and procedures.
- These help ensure management’s direction to mitigate risks so that objectives are achieved and carried out.
- Control activities are performed at all levels of an enterprise, at various stages within business units and processes, and over the technology environment.

COSO Internal Control Components: Internal Control Activities

- These control activities may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.
- A basic or fundamental internal control, segregation of duties is typically built into the selection and development of COSO control activities.
- Where segregation of duties internal controls are not effective or even practical, management must select and develop alternative control activities.

COSO Internal Control Components: Internal Control Activities

- These control activities may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.
- A basic or fundamental internal control, segregation of duties is typically built into the selection and development of COSO control activities.
- Where segregation of duties internal controls are not effective or even practical, management must select and develop alternative control activities.

COSO Internal Control Components: Internal Control Activities

- The revised COSO internal control framework guidance particularly aligns control activities more with the risk assessment element.
- Along with assessing risks, management should identify and put into effect actions that are needed when an enterprise chooses to either accept or avoid a specific risk, and chooses to develop control activities to avoid that risk.

COSO Internal Control Components: Internal Control Activities

- The nature and extent of the risk response and associated control activities will depend, at least in part, on the desired level of risk mitigation acceptable to enterprise management.
- By *mitigation*, we mean some management action that either reduces exposure to the identified risk or the likelihood of its occurrence.

COSO Internal Control Components: Internal Control Activities

- When determining recommended actions to take to mitigate risk, internal auditors should consider all aspects of the enterprise’s system of internal control as well as its relevant business processes, IT systems, and locations where control activities are needed.
- This may include considering control activities outside the operating unit, including shared service, data centers, or processes performed by outsourced service providers. For example, an enterprise may need to establish control activities to address the integrity of information sent to and received from an outsourced service provider.

COSO Internal Control Components: Internal Control Activities - Business Process Control Activities

- Business processes are important areas for internal audit understandings.
- These processes may be common to all business activities—such as purchasing, payables, or sales—or may be unique to a particular industry.
- Each of these processes transforms inputs into output through a series of related transactions or activities. Control activities that directly support actions to mitigate transaction processing risks in an enterprise are usually called *application controls* or *transaction controls*.

COSO Internal Control Components: Internal Control Activities - Business Process Control Activities

- Transaction controls are often the most fundamental control activities in an enterprise since they directly address the risk responses to business processes in place to meet management’s objectives.
- Transaction controls should be selected and developed wherever the business process may reside, ranging from centralized enterprise financial consolidation processes to customer support processes at local operating units.

COSO Internal Control Components: Internal Control Activities - Business Process Control Activities

- A common way to consolidate these business process risks into a manageable form is to group them according to the business process objectives of completeness, accuracy, and availability.
- The control activities element of the COSO internal control framework uses the following information-processing objectives:

COSO Internal Control Components: Internal Control Activities - Information-processing objectives

- Completeness
- Accuracy
- Validity

COSO Internal Control Components: Internal Control Activities - Business Process Control Activities

- **Completeness.** Transactions that occur should be recorded.
- For example, an enterprise can mitigate the risk of not processing all transactions with vendors by selecting actions and transaction controls that support the processing of all invoice transactions within appropriate business procedures.

COSO Internal Control Components: Internal Control Activities - Business Process Control Activities

- **Accuracy.** Transactions should be recorded in a correct amount in the right account and on a timely basis.
- For example, transaction controls over key system elements, such as an item price or vendor master database, can address the accuracy of processing a purchasing transaction. Accuracy in the context of an operational process can be defined to cover the broader concepts of quality, including the accuracy and precision of the recorded part.

COSO Internal Control Components: Internal Control Activities - Business Process Control Activities

- **Validity.** Recorded transactions represent an economic event that actually occurred and then was executed according to prescribed procedures.
- Validity is generally achieved through control activities that include the authorization of transactions as specified by enterprise policies and procedures.

COSO Internal Control Components: Internal Control Activities - Types Of Transaction Control Activities

- The COSO internal control framework guidance material highlights the following types of transaction control activities:
- **Verifications**
- **Reconciliations**
- **Authorizations and approvals**
- **Physical controls**
- **Controls over standing data**
- **Supervisory controls**

COSO Internal Control Components: Internal Control Activities - Types Of Transaction Control Activities

- **Verifications.** This is a transaction type of control that compares two or more items with each other or compares an item with policy rules, and performs a follow-up action when the items compared do not match or are considered inconsistent with policy.
- Examples here include IT applications with programs, including matching or programmed reasonableness tests. Verifications generally address the completeness, accuracy, or validity of processing transactions.

COSO Internal Control Components: Internal Control Activities - Types Of Transaction Control Activities

- **Reconciliations.** This transaction process compares two or more data elements, and if differences are identified, actions are taken to bring the data into agreement. Reconciliations generally address the completeness and/or accuracy of processing transactions.
- **Authorizations and approvals.** An authorization process affirms that a transaction is valid, particularly one representing an actual economic event. An authorization typically takes the form of an approval by a higher level of management or of a system-generated verification and determination that a transaction is valid.

COSO Internal Control Components: Internal Control Activities - Types Of Transaction Control Activities

- **Physical controls.** Equipment inventories, securities, cash, and other assets are typically secured physically in locked or guarded storage areas. The physical control transactions here should be periodically counted and compared with supporting control records.

COSO Internal Control Components: Internal Control Activities - Types Of Transaction Control Activities

- **Controls over standing data.** *Standing data*—a term first introduced some years ago by one of the major public accounting firms—is the data elements developed from outside the enterprise (often from a standards organization) that support the processing of transactions within that enterprise.
- Control activities over the processes to populate, update, and maintain the accuracy, completeness, and validity of this standing data should be established by the enterprise.

COSO Internal Control Components: Internal Control Activities - Types Of Transaction Control Activities

- **Supervisory controls.** These transaction control processes assess whether other transaction control activities, such as verifications, approvals, controls over standing data, and physical control activities are being performed completely, accurately, and according to enterprise policy and procedures.
- Management normally should judgmentally select and develop supervisory controls over higher-risk transactions, including high-level reviews, to see if any reconciling items have been either followed up on or corrected, or to determine whether an appropriate explanation was provided.

COSO Internal Control Components: Information and Communication

- Information is necessary for an enterprise to carry out its internal control responsibilities to support the achievement of its objectives.
- Management obtains or generates and then uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control, and internal auditors review and assess that same management information.

COSO Internal Control Components: Information and Communication

- Communication, the other component of this COSO element, is defined here as the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout an enterprise, flowing up, down, and across the entity.
- It enables personnel to receive clear messages from senior management that control responsibilities must be taken seriously. External communication also enables inbound communications of relevant external information and provides information to external parties in response to requirements and expectations.

COSO Internal Control Components: Information and Communication

- This COSO component describes the importance of the information stored by an enterprise and how it should be communicated to various parties.
- The information system portion of this element records, processes, stores, and reports data. The communication system dictates how information is reported, who gets it, and how it is used in fraud control.
- This information and communication process should:

COSO Internal Control Components: Information and Communication

- Record transactions as they occur, breaking them into their component parts (dates, amounts, names, accounts, authorizations, etc.).
- Process, summarize, and report that information for management purposes and pure accounting purposes.
- Store captured and processed data in formats that can be summarized, audited, reviewed, and reported quickly and easily.
- Report that information in a format that can be used for management analysis and internal control purposes.

COSO Internal Control Components: Information and Communication

- Today we too often think of the term *information* as just an IT issue. However, the COSO internal control framework defines it in a broader sense, stating that information encompasses *all* of the data that is combined and summarized based on their relevance to enterprise information requirements.
- Information systems, as defined by COSO, support decision making by supporting the processing of relevant, timely, and quality information from internal and external sources.

COSO Internal Control Components: Information and Communication

- The COSO communication element component calls for an enterprise to share relevant and quality information internally and externally. Management communicates information internally to enable its personnel to better understand the enterprise’s objectives and the importance of their control responsibilities. Internal communication facilitates the functioning of other components of internal control by sharing information up, down, and across the enterprise.

COSO Internal Control Components: Information and Communication

- External communications enable management to obtain and share information between the enterprise and external parties about risk, regulatory matters, and changes in circumstances, customer satisfaction, and other information relevant to the functioning of other internal control components.

COSO Internal Control Components: Importance Of Using Relevant Information

- With the mass of information which includes an enterprise’s formal published systems and procedures, memos, multiple e-mail communications, external vendor news postings, and communications from social media sources, internal auditors are often bombarded with information when beginning to review and assess internal controls in some area.
- As such an internal auditor should obtain or generate and use relevant, quality information to support the functioning of components of internal control under review.

COSO Internal Control Components: Importance Of Using Relevant Information

- Internal audit, working together as a team with senior management, should be able to survey past operational and financial management results as well as inputs to identify and define better relevant information requirements.
- Obtaining relevant information, as defined in the COSO internal control framework, requires management to identify and define information requirements at a strong level of detail and specificity.

COSO Internal Control Components: Importance Of Using Relevant Information

- The ensuing table shows examples of various types of external and external relevant information in support of the COSO internal control components:

COSO Internal Control Components: Examples Of Relevant Information

Info. Source	Example of Relevant Information	Data Example
Internal	E-mail communications	Organization changes
Internal	Inspection reports from production floor	Online and quality production informaton
Internal	Minutes of notes from operations committee meeting	Actions in response to reported metrics
Internal	Personnel time reporting system	Hours incurred on time-based projects
Internal	Reports from manufacturing systems	Production results: number of units shipped
Internal	Responses to customer surveys	Factors impacting customer repeat purchases
Internal	Whistleblower hotline	Complaints on management behaviors

COSO Internal Control Components: Examples Of Relevant Information

Info. Source	Example of Relevant Information	Data Example
External	Data from outsourced service provider	Products shipped from contract manufacturer
External	Industry research reports	Competitor product information
External	Peer company earning releases	Market and industry metrics
External	Regulatory bodies	New or expanded requirements
External	Social media, blog, or other posts	Opinions about the enterprise
External	Trade shows	Evolving customer interests and preferences
External	Whistleblower hotline	Claims of fraud, bribery, etc.

COSO Internal Control Components: Importance Of Internal Communications

- COSO suggests that an enterprise should internally communicate its objectives and the responsibilities of good internal controls.
- This information-related communication should be initiated and endorsed by senior management and conveyed to all elements across an enterprise organization, including:

COSO Internal Control Components: Importance Of Internal Communications

- The importance, relevance, and benefits of effective internal controls
- The roles and responsibilities of management and other personnel in performing those internal control processes
- The expectations of the enterprise to communicate up, down, and across any matters of significance relating to internal control, including instances of weakness, deterioration, or nonadherence.

COSO Internal Control Components: Monitoring Activities

- Monitoring activities assess whether each of the other five objectives or components of COSO internal control, including the control environment, risk assessment, and others, are present and functioning.
- An enterprise and its internal auditors should use separate evaluation processes to ascertain whether established internal control principles, both across the enterprise and its subunits, are in effect, present, and functioning.
- Monitoring here is a key input into the organization’s assessment of the effectiveness of internal control.

COSO Internal Control Components: Monitoring Activities

- The COSO internal control framework identifies two principles for the monitoring activities' internal control component:
- The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
- 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 Internal Control Components: Monitoring Activities

- Monitoring activities should be selected, developed, and performed to ascertain whether each control component or principle from the five internal control components is present and functioning, and that some forms of internal control deficiencies exist.
- Management also needs to determine whether the system of internal control continues to be relevant and able to address new risks.

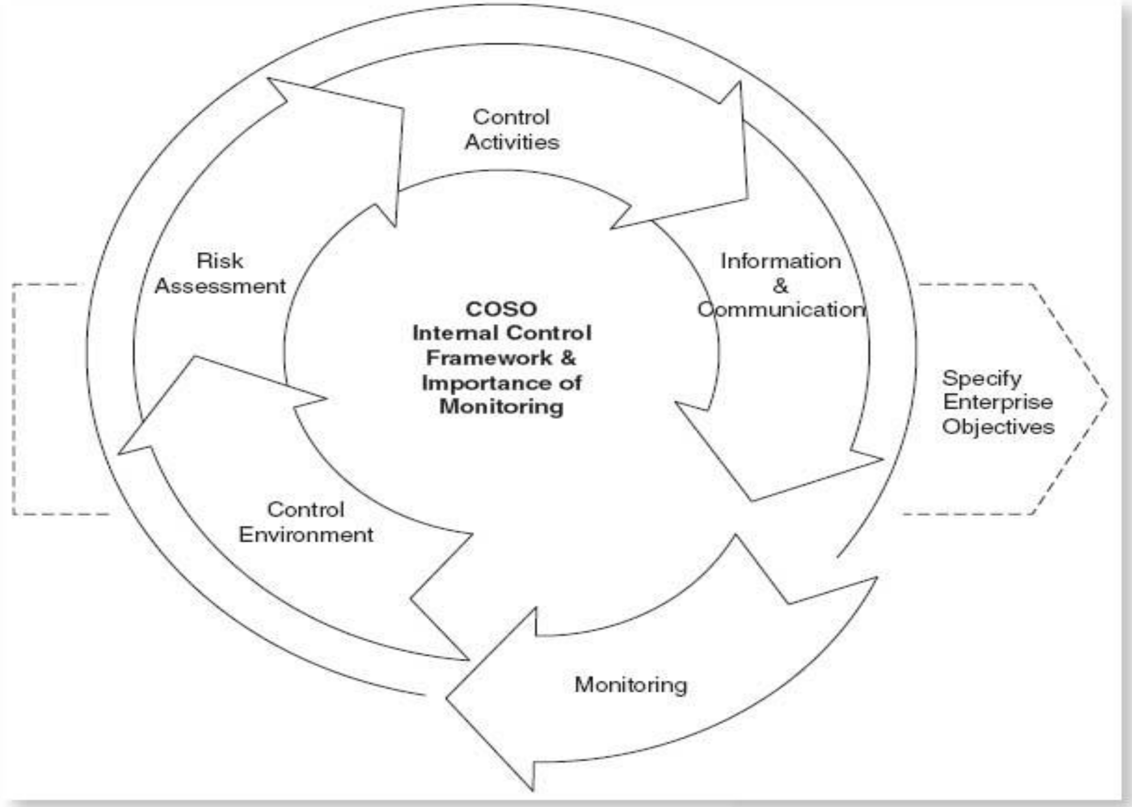
COSO Internal Control Components: Monitoring Activities

- Monitoring activities will generally identify root causes of such breakdowns and may operate within various business processes across the enterprise and its subunits.
- Review activities are not automatically classified as monitoring activities. For example, the intent of a monthly completeness control activity would be to detect and correct errors, where a corresponding monitoring activity would only be to ask why there were errors in the first place, and then to task management with fixing the process to prevent future errors.

COSO Internal Control Components: Monitoring Activities

- In simple terms, a control activity responds to a specific risk, whereas a monitoring activity assesses whether controls within each of the five components of internal control are operating as intended.
- An enterprise should conduct ongoing evaluations to support its monitoring activities and that an enterprise should identify and communicate any known internal control deficiencies as part of its monitoring activities. Installation of appropriate monitoring activities brings to completion a full circle of internal control processes, as illustrated in the following diagram:

COSO Internal Control Components: Monitoring Activities


Control Activities
Risk Assessment
Information & Communication
COSO Internal Control Framework & Importance of Monitoring
Specify Enterprise Objectives
Control Environment
Monitoring

COSO Internal Control Components: Monitoring Activities

The COSO framework defines monitoring as processes to help ensure that internal control continues to operate effectively. When monitoring is designed and implemented appropriately, an enterprise should benefit because it is more likely to:

- Identify and correct internal control problems on a timely basis
- Produce more accurate and reliable information for use in decision making
- Prepare accurate and timely financial statements
- Be in a position to provide periodic certifications or assertions on the effectiveness of internal control

COSO Internal Control Components: Monitoring Activities

- Management and the board of directors should understand the concepts of effective monitoring and how they can serve their respective enterprise interests.
- Internal audit review activities should provide senior management with assurances that their internal control systems are working and that installed monitoring processes are providing that guidance.

Material Taken From

- **Brink's Modern Internal Auditing**
- *Eighth Edition*
- ***A Common Body of Knowledge***

ROBERT R. MOELLER

Material Taken From

The Basics of IT Audit

Purposes, Processes, and Practical Information

Stephen D. Gantz

TECHNICAL EDITOR

Steve Maske