Course: Financial Audit

Lecture 8: Internal Control & Control Risk

Lecturer: Dimaz Ramananda

Overview of Lecture 7

Internal Controls

- Internal control is critical not only for maintaining accurate accounting and financial records but also as a key pillar in the overall governance and management of an organization. These controls serve as a backbone for ensuring accountability across all levels of an entity, from top executives and managers to shareholders, auditors, and even government regulators.
- Globally, the importance of internal control is reinforced through various regulatory frameworks, such as Sarbanes-Oxley (SOX) in the United States, which mandates that management must provide public disclosures about the effectiveness of internal controls in their annual reports.

Internal Controls

- Even companies that appear stable and "in control" face various inherent risks. The presence of effective internal controls does not eliminate risks but helps detect and manage them before they escalate.
- Internal controls play a vital role in such situations by ensuring that the management's responses to these risks are timely, measured, and aligned with long-term organizational goals. This proactive approach minimizes the likelihood of unexpected disruptions or negative financial outcomes.

Internal Controls

- Internal control forms the cornerstone of the audit planning process, particularly during Phase II (Planning) of the Audit Process Model. During this phase, auditors focus on two critical objectives:
  - Understanding the Entity and its Environment
  - Assessing the Risks of Material Misstatements

Internal Controls

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as an ongoing process that is influenced by an entity's leadership, board of directors, and personnel. Its purpose is to provide reasonable assurance regarding:
  - Operational Effectiveness and Efficiency
  - Reliability of Financial Reporting
  - Compliance with Laws and Regulations
  - Safeguarding Assets

Internal Controls

- Internal control is built on a few fundamental concepts:
  - Process
  - People-centered
  - Reasonable assurance

Internal Controls

- Internal control is typically structured around four overlapping categories that together ensure the holistic functioning of the organization:
  - Operations
  - Financial reporting
  - Compliance
  - Safeguarding assets

Internal Controls

- International standards, including those set by the International Standards on Auditing (ISA 315), require auditors to assess risk through a detailed understanding of an organization’s internal controls. They evaluate:
  - Control environment
  - Risk assessment process
  - Information and communication systems
  - Control activities
  - Monitoring

Internal Controls

- Internal controls are critical not just for managing financial accuracy, but also for ensuring operational efficiency, regulatory compliance, and safeguarding the organization’s assets.
- The Chief Executive Officer (CEO) holds the ultimate responsibility and serves as the architect and champion of the control environment. They are tasked with not only designing the internal control system but also ensuring that it is executed effectively.

Internal Controls

- At the board of directors' level, the responsibility becomes one of governance and oversight.
- Board members, through their independent position, are uniquely positioned to identify potential failures in management behavior, such as overriding controls or suppressing communication from subordinates.

Internal Controls

- Additionally, internal controls must be part of every employee's role. This can be explicit, where internal controls are clearly outlined in job descriptions, or implicit, where employees are expected to follow established procedures.
- Ensuring that everyone in the organization understands their part in maintaining internal controls helps create an environment where risks are managed at every level, and accountability is embedded in the company culture.

Internal Controls

- Internal controls serve as a framework through which an organization can achieve three core objectives:
  - Effective operations
  - Accurate financial reporting
  - Compliance with laws and regulations

Internal Controls

- For auditors, internal control systems are a central concern. These systems play a vital role in how they assess the reliability of financial reports. Auditors must determine whether the internal controls are designed and implemented in a way that prevents, detects, and corrects material misstatements.
- By performing detailed evaluations of internal control systems, auditors can:
  - Reduce the extent of substantive testing
  - Enhance the audit’s overall efficiency
  - Provide added value to the client

Internal Controls

- The decision by auditors to rely on an organization’s internal control systems is based on two key factors:
  - Audit efficiency
  - Risk mitigation

Internal Controls

- Auditors often place more emphasis on controls over transactions rather than over account balances or disclosures.
- This is because the accuracy of financial statement outputs (account balances) is heavily dependent on the accuracy of the inputs (transactions).

Internal Controls

- Although auditors primarily focus on financial controls, other controls, such as operational controls and compliance controls, may be relevant to the audit depending on the scope of the work.
- General IT controls, such as restricting access to sensitive financial data through password protection and data encryption, play a significant role in ensuring the integrity of financial systems.

Internal Controls

- To gain an understanding of a company's internal control systems, auditors perform an in-depth evaluation of how these controls are designed and whether they have been implemented.
- An implemented control is one that not only exists on paper but is actively being followed by the organization.

Internal Controls

- Despite their importance, internal controls have inherent limitations. As emphasized by ISA 315, even the best-designed systems can only provide reasonable assurance of achieving the company’s objectives due to various factors:
  - Human error
  - Collusion
  - Management override

Internal Controls

- Internal control is a comprehensive system consisting of five interrelated components that work cohesively to ensure an organization's objectives are met. These components form a structured approach to managing risk, ensuring operational efficiency, safeguarding assets, and ensuring compliance with applicable laws and regulations.
    - Control environment
    - Risk assessment
    - Information Systems, communication, and related business processes
    - Control procedures
    - Monitoring of control

Control Environment

- The control environment serves as the bedrock of an organization’s internal control system, setting the tone for how seriously the organization takes internal control. It encompasses the actions, attitudes, and ethical stance of management and the board of directors.
- The control environment directly influences employee behavior and the overall effectiveness of internal controls. A strong control environment instills a sense of responsibility and accountability throughout the organization, encouraging employees to adhere to policies, procedures, and ethical standards.

Integrity, Ethics & Competence

- The integrity and ethical values of an organization’s people, from top management to entry-level employees, are the pillars of an effective internal control system. Integrity ensures that employees act in accordance with ethical standards, while competence ensures that they have the knowledge and skills to carry out their responsibilities effectively.
- These qualities are essential because internal controls, no matter how well designed, rely on the people who implement them.

Management’s Philosophy

- Management’s philosophy and approach to operations play a crucial role in shaping the organization’s internal control environment
- The behavior exhibited by top management, particularly the chief executive officer (CEO), sends clear signals to employees about the company’s culture and the importance of internal controls.
- Their philosophy can lead to significant risks if they favor aggressive or risky strategies, especially when decision-making is concentrated among just a few key individuals. In this regard, auditors will often assess management’s willingness to monitor business risk and whether they take a risk-averse or risk-seeking stance.

Organizational Structure

- The company’s organizational structure provides a framework for planning, executing, controlling, and monitoring business activities. Key considerations include how clearly lines of authority and responsibility are defined, whether policies and procedures are consistently followed, and how well decentralized operations are monitored.
- The organization’s structure should also align with its size and complexity, as this ensures the proper level of supervision. By examining the structure, auditors can better understand how management oversees various aspects of the business and how control policies are enforced throughout the organization.

Assignment of Authority

- How authority and responsibility are distributed across the organization directly influences the internal control system. This distribution is typically laid out in formal company documents such as policy manuals, which outline business practices, employee responsibilities, and the constraints under which they operate.
- These policies are essential to ensure that only authorized personnel perform certain functions, minimizing the risk of unauthorized transactions or errors. The effectiveness of these controls, however, depends on the extent to which management adheres to these policies. It’s not enough to have a formal code of conduct; management must also practice what they preach. If leadership frequently bypasses these rules or allows exceptions, the entire system of authority and responsibility can be undermined.

Human Resource Policies

- The most critical element of the control environment is the personnel, and this highlights the importance of robust human resource policies. Competent, trustworthy employees can compensate for other control weaknesses, allowing the company to produce reliable financial statements despite any gaps in internal controls.
- Human resource practices such as recruitment, orientation, training, and evaluation are therefore vital in maintaining the integrity of the control environment. Hiring high-quality employees through thorough interviews, assessing their ethical behavior, and evaluating their technical skills helps in building a capable workforce.

Analyzing Control Environment

- When assessing the control environment, it’s important to consider how all the elements work together. Strong areas can offset weaknesses in other parts of the system.
- This interaction between various control elements is critical in determining the overall effectiveness of the system. For instance, strong human resource practices might not be enough to counterbalance a management philosophy that prioritizes short-term earnings over long-term sustainability.

Risk Assessment

- Both management and auditors engage in risk assessment, but their approaches are different, albeit interconnected. Management's risk assessment is geared toward designing an internal control system that minimizes errors and irregularities, while the auditor's risk assessment determines the extent of audit evidence required
- A well-functioning management risk assessment process often results in the auditor needing to collect less evidence since the control risks are lower. Essentially, if management has effectively identified and mitigated risks, the auditor can place more reliance on the company's controls, reducing the need for extensive testing.

Risk Factors

- Risks that affect the organization can arise from both internal and external sources. External risks include technological changes, shifts in customer preferences, new laws or regulations, and economic fluctuations, all of which can force the organization to adjust its operations and strategies.
- Effective risk management requires organizations to be aware of both internal and external risk factors and develop controls that address these potential vulnerabilities.

Business Risks

- Several techniques have been developed to help companies identify and prioritize risks. These methods typically involve assessing which resources are most vulnerable, reviewing past risks, considering new risks posed by changes in objectives or external factors, and continuously anticipating problems and opportunities.
- By taking a proactive approach to risk management, organizations can better prepare for potential disruptions and ensure that they are well-positioned to respond to emerging risks.

Increasing Risk

- Certain conditions inherently increase risk and require special attention. These include changes in the operating environment, the introduction of new technology, rapid growth, new lines of business, or restructuring efforts. Each of these factors can disrupt established controls or introduce new vulnerabilities.
- New technology might bring about unforeseen risks, particularly if employees are not adequately trained or if security measures are not updated to accommodate the new systems.

Flow of Information

- Effective communication is essential for maintaining a strong internal control system. It’s not just about passing information from the top down; communication must flow across all levels of the organization.
- Employees need to understand their roles in the control process and how their activities impact the organization’s overall objectives.

Information Systems

- An organization’s information systems play a vital role in its control environment. These systems include the accounting system, production systems, personnel systems, and various applications for data processing and reporting.
- The quality of information generated by these systems directly affects management’s ability to control operations and produce reliable financial reports. Beyond the data itself, the way information flows through the organization is equally important. Effective communication ensures that employees are well-informed about their responsibilities and how they contribute to the company’s control efforts.

Information Systems

- For an audit, it is crucial for auditors to obtain a comprehensive understanding of the company’s information system and related business processes relevant to financial reporting. This understanding includes several key areas.
- The financial reporting process used to prepare the entity's statements, including significant accounting estimates and disclosures, is another essential aspect of the auditor's review.
- The procedures that guide the flow of transactions from occurrence to their inclusion in the financial statements are fundamental. Many companies rely on IT to automatically transfer information from transaction processing systems to the general ledger and financial reporting systems. While these automated processes can reduce the risk of human error, they also introduce new risks.

Error Resolution

- The auditor must also evaluate how incorrect processing of transactions is resolved.
- The use of IT systems poses specific risks, such as reliance on systems that inaccurately process data or permit unauthorized access. Unauthorized changes to data in master files or failure to make necessary system updates can compromise the accuracy of financial reporting.

Information System Risks

- Risk exists at all levels of the information system, but it is especially critical during the data input phase. Input should only be managed by authorized individuals or systems, and data entry must be accurate, valid, and complete.
- For internal control and documentation purposes, auditors often view the accounting system as a sequence of steps that capture economic events, record them, and assemble them into a ledger before ultimately reflecting them in the financial statements.

Communication

- Another important aspect of the auditor's work is understanding how the company communicates significant financial reporting matters. Effective communication channels ensure that exceptions, errors, and suspected improprieties are promptly reported and addressed
- Open and effective communication channels with external parties are also critical for timely follow-up actions on received communications.

Control Procedures

- Control procedures, also known as control activities, are policies and procedures that help ensure management directives are followed. These procedures are designed to address risks related to the company’s objectives for operations, financial reporting, and compliance.
- Control procedures typically involve a policy outlining what should be done, along with procedures to implement the policy.

Control Procedures

- According to ISA 315, the key categories of control activities are performance reviews, information processing, physical controls, and segregation of duties. Performance reviews are independent checks on activities by individuals not directly involved in the work being reviewed.
- These reviews may include comparisons of actual performance versus budgets, surprise checks, periodic comparisons of accounting records with physical assets, and reviews of functional activity.

Processing Controls

- Information processing control procedures are typically divided into application controls and general controls. Application controls are specific to systems or programs that initiate, record, process, and report transactions.
- General controls, on the other hand, relate to the overall IT environment, ensuring that systems function correctly. These controls include data center operations, system software acquisition, password controls, and security measures.

Maintaining Records

- The company must maintain adequate records for transactions and summarize them correctly. In a manual system, these records may include sales invoices, shipping documents, purchase orders, journals, ledgers, and time cards.
- In computerized systems, these records are stored in the database of an accounting application. Regardless of the system used, records should be adequate to ensure that assets are controlled and all transactions are recorded accurately.

IT Controls

- General IT controls ensure that access to systems is restricted to authorized individuals. Proper delegation of authority defines the acceptable level of risk and determines the authorization limits for employees. Authorization may be general, as in preset product price lists, or specific, as in individual price reductions for defective items.
- Physical controls are also critical for securing assets. These controls may include locks on storerooms, safes for valuable items, and fireproof cabinets for important records. In computerized environments, physical access controls protect hardware, while backup and recovery procedures safeguard data.

Segregation of Duties

- Segregation of duties is designed to reduce the risk of errors and prevent inappropriate actions. It ensures that responsibilities for authorizing, recording, and handling assets are divided among different people.
- This separation of responsibilities helps ensure that no single individual has control over all aspects of a financial transaction, which minimizes the risk of fraud or error.

Conclusion & Closing

Lecture 8: Internal Control & Control Risk

Lecturer: Dimaz Ramananda

Reference (reading material):

- Principles of Auditing: an Introduction to International Standards on Auditing, 3rd Edition, Hayes, Wallage, and Gortemaker, Pearson Education Limited, 2014