Internal Controls

Lesson 3

KEY CONCEPTS

■ Internal Control ■ Internal Check ■ Preventive Control ■ Detective Control ■ Input Control ■ Output Control ■ Risk Management

Learning Objectives

To understand:

- The meaning & definition of Internal Control
- Objectives, dimensions and types of Internal Control
- What are the Difference between Internal Check and Internal Control
- What are the benefits and limitation of Internal Control
- The various internal control techniques
- Internal control frameworks prescribed by COSO, Cadbury committee
- Role of internal auditors in implementation of internal controls
- How to examine the effectiveness and efficiency of internal controls
- Fraud risk awareness
- Risk Management, Types of Risks, Enterprise Risk Management, Risk Management Plan
- Recommend internal controls to prevent and detect fraud and educate to improve the organisation's fraud awareness
- What are the role of Internal Control in the New Digital ERA such as Robotic Process Automation (RPA), Artificial Intelligence and Machine Learning, Block chain Technologies, Cloud Computing

Lesson Outline

BACKGROUND

To understand the internal controls, it is important to understand the relationship which exists between the directors or those charged with governance (TCWG), the members (or shareholders) of a corporate entity be it a private company or a public company or Section 8 company of the Companies Act, 2013 ("the Act") and the auditors (statutory and internal) for it is relevant to the object and significance of an audit of such a company.

A company is in law regarded as a separate legal entity independent from its members. (Salomon v Salomon & Co. Ltd. (1897). However it has no physical existence, neither soul nor a body of its own. The company itself cannot act in its own person, it can only act through directors. The board of directors are the brain of the company and the company can and does act only through them.

In view of the above, the directors of the company are appointed by the members to manage their company and the Act has set out their responsibilities for ensuring that the company keeps proper financial and non-financial records and for presenting audited annual accounts to the members.

However, in practice the day to day running of the company and the work of keeping and maintaining appropriate financial and non-financial records commensurate with the size and nature of business is often delegated by the directors to the employees.

The directors can discharge their responsibilities by instituting adequate internal controls and internal checks to ensure that this work is carried out properly by the employees. The directors can then rely on this system for the production of reliable management information, financial records, cost accounting records etc. and to prevent errors, frauds and loss of the company's assets.

The responsibility for safeguarding an organization's assets, maintaining proper records and preventing and detecting errors and frauds rests with the directors or those charged with governance. The members or other stakeholders must look to the directors or those charged with governance and not the auditors for the effective discharge of this duty.

As per the provisions of the Act, the board of directors may delegate certain of their responsibilities relating to maintenance of financial and non-financial records and systems of internal controls, review of interim financial statements and annual financial statements to an "audit committee". Audit committee may comprise of both executive and non-executive directors as prescribed under the Act in according to size and nature of its business.

Even in the case of non-corporate entities, not-for-profit organisations, internal control plays a vital role in running a sustainable enterprise.

MEANING OF INTERNAL CONTROL

Internal controls are the mechanisms, rules and procedures implemented by an entity to ensure the integrity and reliability of financial and non-financial records, management information and cost accounting records, promote accountability, prevent and detect errors and frauds. The auditors also rely on the system of internal control for the purpose of audit of the financial accounts.

Internal control comprise internal accounting controls and operational controls. The auditors are primarily concerned with internal accounting controls.

Basic controls include features like control accounts and numerical controls to ensure that all transactions are completely accounted for in the books of account. Disciplines over basic controls include the segregation of incompatible duties, segregation of custody of assets from the accounting responsibilities, physical safeguards to prevent unauthorised access to assets or accounting and other sensitive records and internal check.

DEFINITIONS OF INTERNAL CONTROL

As per Section 134 of the Companies Act, 2013, the term "Internal Financial Controls" means the policies and procedures adopted by the company for ensuring, orderly and efficient conduct of business, including

adherence to company's policies, safeguarding of its assets, prevention and detection of frauds and errors, accuracy and completeness of the accounting records, and timely preparation of reliable financial information.

Committee of Sponsoring Organizations of the Treadway Commission **(COSO)** defines 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 relating to operations, reporting, and compliance."

The Institute of' Chartered Accountants of England and Wales defines Internal Control as "Internal Control means not only internal check or internal audit, but the whole system of control, financial and otherwise, established by management in order to carry on the business of the company in an orderly manner, safeguard its assets and secure as far as possible accuracy and reliability of its records".

De Paula defines, "internal control as system of controls, financial and otherwise, established by management in order to carry on the business of the company in an orderly and efficient manner, safeguard the assets, secure as much as possible the completeness of an internal control system".

Definition as per International Standard on Auditing 315

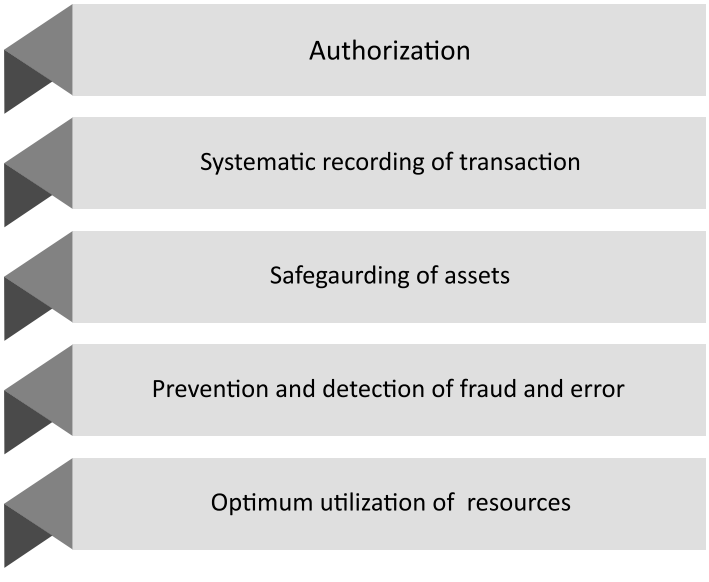
Internal Audit as "the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations". The term "controls" refers to any aspects of one or more of the components of internal control.

Definition of control as per the Institute of Internal Auditors, USA (IIA)

Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Gibbins, [1990]; argues that internal controls may be incorporated with in computerized accounting system, which extends beyond those matters which are related directly to the accounting system.

OBJECTIVES OF INTERNAL CONTROL



- To ensure that the business transaction takes place as per the general and specific authorisation of the management. Ensuring all the authorised transactions are recorded in the financial and non-financial records.
- To ensure that there is a systematic recording of every transaction completely, sequentially with the accurate amount in their respective account and in the correct accounting periods in which they occur as per generally accepted accounting principles and accounting standards.
- To safeguard the entity's assets from unauthorised use with the help of physical security systems, anti-theft devices like RFID, burglar alarms and cameras etc.
- To compare the assets both current and non-current as per the records with that of the physical assets at regular intervals and report to TCWG, in case any difference is found.
- To review the working of the organization and the loopholes in the operations and take necessary steps for its correction.
- To ensure there is the optimum utilization of the entity's resources.
- To find out whether the financial statements are in alignment with the accounting standards and generally accepted accounting principles.

Players in the Internal Control Frameworks

Accounting and Finance Department, Internal audit professionals are the key players along with the other departments in the internal control frameworks of their entity. In today's rapidly changing, technologically disruptive world with artificial intelligence, robotic process automation, machine learning etc., entities across the world face many challenges grappling with Big Data. Data-driven insights enable management to act and react quickly and take decisions as appropriate.

With a strong commitment to trust and ethics effective internal control system require a combination of people, process and technology and data driven entity.

DIMENSIONS OF INTERNAL CONTROL

As per Foreign Corrupt Practices Act, 1977 of United States of America, accounting provisions require issuers (both U.S. and non-U.S. companies that are publicly traded in the United States) are required to establish and maintain a system of internal controls sufficient to assure that

(i) transactions are executed in accordance with management's authorization;

(ii) access to assets is permitted only with the proper authorization; and

(iii) the accounting records reflect the existing assets.

Later in the year 1985, COSO began as a private sector initiative to investigate the causal factors that lead to fraudulent financial reporting as a result of a number of accounting scandals that emerged in the 1970s and mid-1980s.

This initiative was termed the National Commission on Fraudulent Financial Reporting. The first president of the Commission was James C. Treadway, Jr., a former Commissioner of the US Securities and Exchange Commission, and therefore the initiative was commonly called the **"Treadway Commission".**

One of the major factors that influences a business organisation to adopt internal control is to provide a reliable financial statements to its stakeholders especially in this start-up era.

CASE STUDY

A firm with two partners who take active part in running the vegetable business, with two assistants. The firm has a simple accounting system and does not need more than a cash and bank book to record. Expenses such as rent and insurance, Purchase of vegetables like cabbages, carrot, potatoes, onion etc. Sale of vegetables etc.

The expenses and purchases are supported by two box files of "paid" and "unpaid invoices" and they have billing machine to record sales.

As an internal auditor how would you ensure that sales and purchases were completely and accurately recorded?

Solution:

The following controls would be helpful in ensuring that sales and purchases were fully and accurately recorded by the company in vegetable selling business.

Purchases

1. Since some of the vegetables have limited shelf life, purchases of stock are to be made by the partners of desired quantity and quality to avoid wastages.
2. Invoices to be numbered on receipt of goods to ensure that all purchase invoices are filed in the invoice files. This control is backed up by periodic sequence checks.

   [A sequence check is a check to ensure that a sequence of numbers is complete. For example if purchase invoices in the file contains 1,2,3,5 and 6, invoice number 4 can be seen as missing and steps shall be taken to recover it.]

Sales

1. Personal supervision of the two assistants by the partners, at least one partner has to be in the shop during opening and closing hours since most frauds are perpetrated at this time.
2. Comparison by the directors of actual sales with expected sales on a weekly basis.
3. Comparison of actual and expected gross margin on a monthly basis.

Accounting controls: The basic accounting system and such controls as the use of accounting information to detect variances from expectation (comparing of actual sales with expected sales) and those that ensures that records are complete using sequence checks.

Administrative controls: Non-accounting controls such as the personal supervision by the partners and restriction of purchasing to the partners.

Consider the way in which purchase invoices are numbered and filed. The numbering makes it more likely that all transactions have been recorded, the sequence check strengthens this control and also aids detection of errors and/or frauds. Considering the size of business, segregating of purchase invoices in two different files as paid and unpaid enables outstanding creditors to be easily established.

Safeguarding of assets : An important control in the vegetable shop to safeguard the assets (cash and vegetable stock which are highly susceptible to theft) is that of close supervision by the partners.

Partners personally purchase the produce to be sold, this control is to ensure that management policy of selling a particular grade of vegetables is being adhered to.

The carrying on of the business in an efficient and orderly manner can be exemplified by the use of accounting information to enable the partners set the prices of the vegetables.

A proper record of purchase cost of vegetables would be a prerequisite for setting sale price.

Difference between Internal Check and Internal Control

Internal Check can be defined as a method or an arrangement of the operations of a factory, office, warehouse, store, etc, in a manner that the work of one employee automatically comes under the scrutiny of another employee, so as to minimize the risk of errors and frauds.

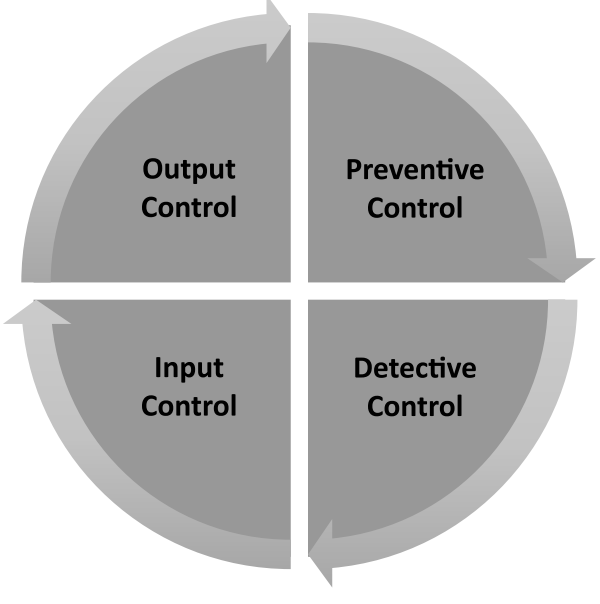
Internal Check	*Internal Control*
It is a method of arranging the operations of an enterprise wherein the work of one employee is automatically checked by another employee to minimise the risk of error and fraud.	It is a whole system of controls financial and otherwise established by the management.
Scope of internal check is very limited and in the case of small enterprises it is practically difficult.	Scope of internal control is very wide, it includes internal check and internal audit.

TYPES OF CONTROL

There are preventive, detective, physical and logical controls in all entities commensurate with its size and nature of its business.

Examples of internal controls are internal audits, firewall deployment, training, and employee disciplinary procedures. All organisations are subject to various risks that might harm the organization and could result in asset loss, reputation loss and so forth. From unintentional mistakes to fraudulent manipulation, risks are present in every business.

The importance of internal controls lies in their ability to protect the organization from risks and the consequences thereof. For example, IT security controls reduces the risk of data breaches or malware infection. It helps to find weak spots in information systems and then strengthen those weak spots. Internal controls have its limitation on what it can accomplish; hence it is essential to have an ongoing reviews and monitoring of existing internal control system.



1. Preventive Control

We have heard many times that "prevention is better than cure". Preventive internal controls are put in place to prevent an adverse event from occurring. For example, many software applications have built-in checks and balances to avoid entering incorrect information.

Preventive controls are the best kind of controls because they lessen the need to detect errors and fraud after it has occurred. Automated preventative controls are even better because they remove the need for human intervention. They are proactive in nature that assists the management to ensure that strategic and departmental objectives are achieved.

Examples of Preventive Internal Controls

Segregation of duties, Rotation of duties, background verification of employees, prior approvals, authorisation and verification, firewalls, computer and server backups are all preventive internal controls that block undesirable events from occurring.

Background screening for employees:

Background screening is a procedure where employers check candidates' backgrounds, screen them for drugs, check references, and assess their conduct. It is used in the recruiting process to screen out many undesirable candidates before investing in the onboarding process. Many a frauds can be prevented by this process.

2. Detective Controls

Detective internal controls detect an error or fraud after it has occurred. Ideally, detective internal controls will discover an issue before it becomes a significant problem. It is more of a post mortem exercise.

Examples of detective controls are internal audits, reconciliations, financial reporting, financial statements, and physical verification.

3. Input Controls

Input controls in the context of internal control means the procedures and systems to ensure completeness, accuracy, existence, validity of the data entered in the financial and non- financial records. Input control helps in preventing errors and frauds thereby making the information is reliable for decision making.

Examples are: Data validation, Data verification, Audit trail and authorisation procedure.

4. Output Controls

Output controls in the context of internal control means the mechanism put in place to monitor and evaluate the results of operation or activities. The purpose of output control is to ensure that the objectives of the entity are met and the results are in line with the expectations.

Examples are: Monitoring and measuring key performance indicators such as productivity, efficiency and effectiveness, quality control, obtaining feedback, review of exception reports.

INTERNAL AUDIT & INTERNAL CONTROLS

The objective of an internal audit is to evaluate compliance with company procedures, applicable laws, and international standards. Data and reports are reviewed to assure consistency and compliance. This internal control provides a value-added service to management and to the board of directors by detecting and correcting weaknesses in a process before external audits discover them. This can protect the organisation from loss of reputation and regulatory fines.

1. **Periodical reconciliations and financial reporting:** Reconciliations are performed to verify financial reporting among various sources. For example, comparing (or reconciling) a bank statement or debtors statement of account to a company's internal records is one form of reconciliation.

   Financial reporting discloses the entity's revenues, expenses, cash flow, and financial health. It allows executives and investors to make more informed judgments on performance and opportunities for improvement. Unusual or unexpected variances in financial statements helps to detect inadvertent errors and intentional fraud.

2. **Physical verification:** Physical verification of tangible assets is performed periodically to assure actual count of assets (inventory, property, plant and equipment, investments, cash etc) match what is recorded in business systems and financial statements. Physical assets values directly affect the balance sheet, so it's vital they are reflected accurately. Discrepancy investigations can reveal system issues, inadvertent errors, and possibly embezzlement or theft. This is helpful at remote locations like branches, manufacturing facilities, warehouses, projects.

3. **Corrective Internal Controls:** Corrective internal controls are implemented after the internal detective controls discovers a problem. These controls could include disciplinary action, report filing, software patches or modifications, and new policies. They are usually put into place after a root cause investigation.

   Examples of Corrective Internal Controls

   Corrective internal controls, by nature, are specific to the typical flaws and risks of the company, previously evaluated through comprehensive risk assessments or detective controls, such as audits.

4. **New or Updated Policies and Procedures:** Policies and procedures needs to be updated when an audit or other detective control identifies a gap in processes or if new Enterprise Resources Planning software is implemented. For example, root cause analysis on a physical inventory discrepancy may reveal that employees are inadequately trained on how to account for the parts that fail quality checks. Corrective controls would include updated work instructions and training.

5. **Disciplinary Actions:** Disciplinary actions are corrective actions taken in response to employee misbehavior, rule violations, or poor performance. Discipline can take several forms depending on the seriousness of the situation, including a verbal warning, formal warning, an unfavorable performance evaluation, or even termination.

BENEFITS AND LIMITATIONS OF INTERNAL CONTROLS

Processes and control activities are imperfect, and errors and problems will inevitably be found. Therefore, an ongoing review and analysis of internal controls should be a part of any organization's regular processes.

Benefits of Internal Controls

Management is ultimately responsible for the control environment and the success of internal controls. The benefits of internal controls depend upon correct implementation and ongoing monitoring.

1. **Early Warning System:** Internal controls serve as an early warning system to identify issues before they become big problems. Quality checks prevent faulty products from being shipped to customers. The investigation into a slip in on-time delivery metrics may reveal a more significant problem on the horizon. Problems are easier to fix when you catch them early.

2. **Prevent Fraud:** Robust internal controls deter employees from engaging in misconduct. When employees can see process gaps, they may be tempted to perform minor inappropriate actions that

eventually lead to major ones. With multiple checks and balances, however, fraud is much more difficult. Solid policies assure that employees understand the consequences.

3. **Avoid External Audit Findings and Regulatory Fines:** Performing investigations and corrective actions on external audit findings can be a laborious process. If an external audit identifies a significant gap in processes or material misstatements, entity could be exposed to losing industry certifications or substantial fines. It is always best to find and fix a problem before an external entity discovers it.

   If an entity still experience a data breach, robust internal controls can also protect it from hefty fines. If an investigation reveals that the entity acted with due diligence and had adequate controls in place, a regulatory agency may reduce penalties.

Limitations of Internal Controls

Despite the benefits, internal controls have some limitations. It's crucial to be aware of the gaps left by internal controls to assure that those risks are understood.

1. **Collusion (Override a control):** Segregation of duties is one of the most prevalent internal controls businesses use. It separates tasks so that no one employee has the power to commit fraud. Employees can, however, get past this by collaborating together in an elaborate process to disguise their fraud. Collusion involves two or more employees agreeing to take common action to override a control.

   For example, employee A is the warehouse manager in charge of stock and another employee B from accounts department is required to count stock and compare it with stock records. A misappropriates stock and B is aware of it and helps A by falsely reporting that there are no discrepancies between stock records and physical count. This is a clear case of Collusion.

2. **Human Error:** Human error can be another disadvantage of internal controls, especially when relying on manual processes and judgment calls. For example, inadvertent errors can be made during manual inventory counts, and poor judgment could impact internal audit results. Wherever possible, automated systems should be employed to drive consistency and reduce human error.

   For example, weighing scales along with CCTV cameras can be used in stockrooms to verify inventory counts. Automated systems can help perform reconciliations among accounting and financial records. Solid auditing processes, along with management oversight, will support rigorous internal auditing standards.

3. **Unforeseen Circumstances:** Internal controls rely on a company's management anticipating all potential hazards and implementing mechanisms to prevent or mitigate them. Still, management cannot anticipate all potential challenges or events. Random variables or occurrences are prone to render internal controls ineffective.

   Moreover, attempting to control unusual conditions can be costly, and a management team may instead choose to accept the risk. For example during lockdown time during pandemic employees were working remotely from their home. As a result, internal controls may be limited in their use under unexpected or extraordinary scenarios.

   Apart from risk assessments, procedures, reporting, and communication, the only thing that all internal control schemes have in common is detailed documentation and reporting.

   Small companies may begin by managing their controls with spreadsheets, but the number of internal and external stakeholders increase as their business grows. As a result, preparing ahead of time can save time and money in the long run by having latest version of software appropriate to the size and nature of business.

4. **Internal Controls in Smaller Entities:** Fewer employees limits the extent of segregation of duties but if owner –manager has effective oversight it may compensate to some extent. Overriding of controls by owner-manager is a significant risk because the system of internal control is less structured.

INTERNAL CONTROL TECHNIQUES

1. **Segregation of Duties:** Separation of duties is a critical internal control designed to reduce the incidence of error or fraud by assuring that no single employee has the potential to both perpetrate and hide errors or fraud in the course of his or her activities. Assigning one person to write cheques and another staff member to authorise the payments is one example of segregation of duties. In general, the primary incompatible responsibilities that must be separated are Performing transactions, Authorisation or acceptance, Reconciliation, Asset custody.

2. **Access Controls:** Access controls ensures who has or what has access to corporate assets, including IT systems. These controls are a crucial security concept that reduces risk to the company or organisation. Limiting access to sensitive information and systems only to authorised personnel.

   Physical access control limits access to manufacturing areas, buildings, vital installations, and physical IT assets. Security guards verifying ID credentials or access key cards or biometric access (facial recognition or thumb impression) may be employed to enforce physical access control. Common security measures that prevent physical access in smaller entities are locks, burglar alarms and cameras.

   Physical controls also includes indirect access via documentation. It refers to the fact that the use of inventory needs to be controlled and the inventory should be released only if it is authorised. It will be meaningless to keep inventory in a locked area if anyone can obtain as much as they want without any authorisation.

   Logical access control restricts connections to computer networks, system files, and data. The principle of the least privilege is an information security standard that says users should only access system functions and data that are necessary for the user to do his or her job.

3. **Auditing:** Regularly reviewing and assessing internal controls, processes, and systems to identify and address any issues or weaknesses both by the internal auditors and external auditors.

4. **Risk Management:** Identifying, assessing, and managing potential risks that could impact the organization's objectives.

INTERNAL CONTROL FRAMEWORKS (COSO, CADBURY)

COSO Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a private sector organization that provides guidance on internal control, including enterprise risk management and financial reporting. The COSO framework is widely recognized as the leading framework for internal control and provides a systematic and disciplined approach to risk management.

It provides a systematic approach for organizations to assess and improve their internal controls, with the goal of reducing the risk of fraud and other financial misstatements.

The COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control Framework is a widely recognized framework for assessing and improving the internal controls of an organization. It was first published in 1992, and the latest version was released in 2012.

The COSO Internal Control framework 2012 consists of five (5) interrelated components of internal control and seventeen (17) principles: Control environment, risk assessment, control activities, information and communication, and monitoring.

1. **Control environment** sets the tone for the organization and is the foundation for the other components. This component involves the tone at the top, the integrity and ethical values of the organization, and the way the organization manages risk.
2. **Risk assessment** component helps organizations identify, assess and prioritize the risks they face in achieving its objectives.
3. **Control activities** refer to the policies and procedures that are put in place to mitigate those risks.
4. **Information and communication** ensure that the necessary information is recorded, processed, and communicated effectively to support other components of internal control.
5. **Monitoring** refers to the ongoing assessment of the internal control system to ensure that it remains effective and relevant and communication of results to those charged with governance.

The updated COSO internal control framework 2012 provides guidance for organisations to assess and improve their internal control systems, with a focus on the achievement of objectives in the categories of operations, financial reporting, and compliance with laws and regulations. It is widely used by auditors, internal control professionals, and management to improve the effectiveness and efficiency of internal control systems.

Control Enviornment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Morning Activities	16. Conducts ongoing and/or separate evaluation 17. Evaluates and communicates deficiencies

Control Environment

1. The organisation demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organisation demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organisation holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. Identification and assessment of risks relating to objectives.
7. The organisation identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organisation considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organisation identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

10. The organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organisation selects and develops general control activities over technology to support the achievement of objectives.
12. The organisation deploys control activities through policies that establish what is expected and procedures that put policies into place.

Information and Communication

13. The organisation obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organisation communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

16. The organisation selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organisation 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.

Cadbury Committee of United Kingdom

Sir George Adrian Hayhurst Cadbury was a British businessman and member of the Cadbury family. He is known for his role as chairman of the Cadbury Committee, which produced a report on corporate governance in 1992.

The Cadbury Committee, also known as the Financial Reporting Council (FRC), was established in 1991 in response to a series of corporate failures in the United Kingdom. It was formed in 1991 in the United Kingdom and was charged with reviewing the role and effectiveness of corporate governance in UK companies.

The Cadbury Report, which was published in 1992, established a set of principles for corporate governance and helped to raise the standards of corporate governance in the UK. The Cadbury Report was a landmark publication that set out principles for good corporate governance and helped to shape the modern understanding of corporate governance.

The Cadbury Report emphasized the importance of transparency, accountability, and independent oversight in corporate governance. It also introduced the idea of the board of directors being responsible for setting the tone at the top and setting the company's values and ethical standards.

The Cadbury Report had a significant impact on corporate governance practices in the UK and beyond, and its recommendations continue to be influential to this day. Both the COSO and Cadbury frameworks provide important guidance for organizations looking to improve their internal controls and governance practices. The COSO framework focuses specifically on internal control, while the Cadbury Report addresses broader issues of corporate governance. Both COSO and Cadbury are important references for internal control and corporate governance.

The COSO framework provides a comprehensive approach to internal control and risk management, while the Cadbury Report provides principles for effective corporate governance. Both frameworks continue to be widely used and are considered best practices for organisations looking to improve their internal control and governance processes.

SOX and Internal Controls over financial reporting (United States of America)

The Sarbanes-Oxley Act (SOX) was enacted in 2002 in United States of America in response to a number of high-profile accounting scandals, such as Enron and WorldCom that caused a loss of investor confidence in the reliability of financial reporting. The fundamental objective of this law was to protect the interest of investors by imposing new rules on accounting and financial transparency.

SOX was designed to restore public trust in the financial reporting of publicly traded companies by improving the accuracy and reliability of financial statements, strengthening internal controls, increasing transparency, and enhancing corporate governance.

The SOX seeks to prevent fraudulent financial reporting and corporate accounting irregularities by imposing stricter regulations and penalties on companies and their executives.

The Sarbanes-Oxley Act (SOX) requires companies to establish and maintain internal controls over financial reporting to ensure the accuracy and reliability of their financial statements. These controls are designed to prevent fraudulent financial reporting, provide reasonable assurance that financial information is complete and accurate, and safeguard company assets.

SOX mandates that the management of a company assess the effectiveness of its internal controls and provide an annual report to external auditors. Additionally, external auditors are required to review and attest to the effectiveness of a company's internal controls.

Steps for Establishing Internal Control

- Identify the key areas where the internal control system is to be established.
- Work flow should be designed in such a way that it is not complete if another person has not checked it. (Maker/ Checker concept)
- Establishing of surprise check mechanism where money plays a significant role. Example cash verification, inventory and other high value documents like title deeds.
- Review of units and facilities which are in remote locations.
- Reporting mechanism for non-adherence of key compliance areas.
- Vigil mechanism for larger entities as applicable.

ROLE OF INTERNAL AUDITORS IN IMPLEMENTATION OF INTERNAL CONTROLS

Internal auditors play a critical role in the implementation of internal controls. They provide assurance that internal controls are designed and operating effectively, and help identify areas where improvements can be made. Some key responsibilities of internal auditors in the implementation of internal controls are:

Assessing risk: Internal auditors assess the risks facing an organisation and make recommendations for controls that can mitigate these risks.

Evaluating existing controls: Internal auditors evaluate existing controls to determine their effectiveness and make recommendations for improvement.

Recommending controls: Internal auditors recommend new controls to address areas where risks are high and existing controls are not adequate.

Monitoring implementation: Internal auditors monitor the implementation of new and existing internal controls to ensure that they are operating effectively. They also perform regular follow-up audits to ensure that the recommended improvements have been made and that the control system remains effective.

Reporting: Internal auditors provide regular reports to management on the status of internal controls. Internal auditors communicate their findings to management and other stakeholders, including the board of directors. They provide recommendations for improving the control system and make suggestions for enhancing overall risk management. They identify any weaknesses or deficiencies in the control system and make recommendations for improvements.

Supporting compliance: Internal auditors support the organisation's efforts to comply with laws, regulations, and standards by evaluating the effectiveness of compliance controls.

Evaluating control design: Internal auditors evaluate the design of the internal control system to ensure it is effective and efficient. They review the documentation of the control procedures to determine if they are adequate to meet the company's objectives.

Testing control effectiveness: Internal auditors test the effectiveness of the internal control system by conducting audits and other evaluations.

The internal auditor should be familiar with STANDARD ON INTERNAL AUDIT (SIA) 11 "Consideration of Fraud in an Internal Audit" issued by the Institute of Chartered Accountants of India while conducting Internal Audit of any entity.

Providing training: Internal auditors provide training to employees on the importance of internal controls and how they can be used to support the organisation's goals and objectives.

EXAMINE THE EFFECTIVENESS AND EFFICIENCY OF INTERNAL CONTROLS

Internal controls are measures put in place by organizations to ensure the reliability of financial reporting, promote efficiency and effectiveness in operations, and compliance with laws and regulations. The effectiveness and efficiency of internal controls can be evaluated by examining several key aspects:

1. **Design:** The design of internal controls must be appropriate to address specific risks and must be able to effectively mitigate those risks. The controls should be designed in a way that does not create unnecessary complexity, which could lead to inefficiencies in the operations of the organisation.
2. **Implementation:** The internal controls must be properly implemented and be an integral part of the organisation's operations. This means that employees must be trained on the controls and be familiar with the procedures they need to follow.
3. **Monitoring:** The internal controls must be regularly monitored to ensure they are functioning as intended. This includes regular audits and reviews of the control environment to identify any weaknesses and make improvements as needed.
4. **Documentation:** Proper documentation of internal controls is essential to ensure that they are consistently followed and that any changes to the controls are properly recorded.
5. **Evaluation:** Periodical evaluation of the effectiveness and efficiency of internal controls is critical to ensuring they remain relevant and effective in mitigating risks. This includes ongoing monitoring and assessment, as well as periodic internal audits or external reviews. By regularly evaluating and improving the controls, organizations can ensure that they are able to operate effectively and efficiently, while minimizing risks to the organization and its stakeholders.

FRAUD RISK AWARENESS

Fraud risk awareness refers to the understanding and recognition of potential fraudulent activities that could harm an individual or an organization as well as the measures that can be taken to prevent or mitigate them. It encompasses being able to identify red flags and warning signs, understanding how fraudsters operate and taking proactive steps to mitigate potential losses.

Fraud can occur in various forms, including financial fraud, cyber fraud, identity theft, and more. By being aware of fraud risks is crucial in order to prevent or detect such activities and minimise the damage caused by fraud.

There are several steps that individuals and organizations can take to increase fraud risk awareness:

1. **Stay informed:** It is important for individuals and organizations to regularly assess and update their fraud risk awareness efforts to stay ahead of evolving threats. This can be done by staying informed about the latest fraud schemes, tactics and trends used by fraudsters, and implementing best practices for fraud prevention.
2. **Be vigilant:** Be cautious of any unusual or suspicious behavior and report it promptly.
3. **Protect personal information**: Keeping sensitive information such as social security numbers, bank accounts, and passwords secure and private.
4. **Implement security measures:** Using strong passwords, enable two-factor authentication, and install antivirus software on devices. Keep passwords secure and unique, and change them regularly.
5. **Train employees:** Educate employees on the latest fraud trends and how to recognize and prevent fraud.
6. **Monitor accounts regularly:** Regularly review bank and credit card statements and monitor accounts for any unusual or suspicious activity.

    - By being aware of the potential risks and taking proactive measures, individuals and organizations can reduce their vulnerability to fraud.

- Be cautious of unsolicited emails and phone calls, especially those that ask for personal information.
- Using strong anti-virus and anti-malware software to protect computer systems.
- Avoiding using public Wi-Fi networks for sensitive transactions, such as online banking.
- Be wary of too-good-to-be-true offers or deals that are not from a trusted source.

Fraud risk awareness is a critical aspect of protecting oneself and one's assets. By staying informed and taking proactive measures, individuals and organizations can reduce the risk of falling victim to fraudulent activities.

Understanding and documenting the system

Any entity be it a small entity, a large enterprise, a multinational company, Government, Bank, Insurance Company, Not for Profit organisations like Trust, Charitable Institutions need an adequate accounting system. This will enable them to control the business, safeguard the assets, prepare accounts and comply with legislation of the land. Hence, it is fundamental in order to carry out an effective internal audit or statutory audit, the auditor should gain an understanding of the existing accounting system and of the procedures and controls incorporated therein, sufficient for the purpose of his audit.

It is considered preferable that the processes necessary to understand and document the entity's accounting system and to evaluate the entity's system of internal controls to be conducted separately. It is then easier for the internal auditor to keep clearly in mind the differences involved in these two phases.

The documenting of the understanding of an entity's accounting system may be achieved as below:

1. An extended form of internal control questionnaire
2. Notes on accounting procedures or other narrative description
3. Flow charts.

For small business, certain of the procedures may not be appropriate. When reliance is not to be placed on internal controls, the auditor may only need brief notes of the clients' accounting system. A small business with few staff operating from one location might not warrant the preparation and completion of internal control questionnaires or flow charts.

Where the accounting system is complex, it is preferable for the internal auditor to use flowcharting techniques in conjunction, if necessary, with narrative descriptions to record his understanding of the system since flowcharting enables the auditor to obtain a better understanding of the system and to identify more easily the relevant control features in the system.

After having completed the flowcharts or notes on accounting procedures to document his understanding of the entity's accounting system, the auditor should confirm the understanding by carrying out a transaction review by way of walk-through test.

Transaction reviews: The transaction reviews should be documented, showing the operations reviewed and identifying the specific transaction selected. The results of the transaction review may conveniently be filled with the related flowcharts or notes on accounting procedures.

Narrative Description: The internal auditor prepares a written description of the system in use.

Internal Control Questionnaire: The internal auditor considering the size and nature of its business and based on the discussions with the management designs a set of questions, which when answered will document a number of aspects of the internal control system. This questionnaire is popularly known as internal control questionnaire (ICQ) and can be very useful in documenting and assisting the evaluation of controls.

Visual description: The internal auditor uses charts to make the system more visual and easier to understand. Organisational Chart, Audit trail flow chart (cradle to grave),Document flow chart and Systems flow chart used in documenting computer systems as application controls.

CASE STUDY

Pink collar crime – Largest municipal fraud in the history of United States

Rita Crundwell was a controller and treasurer of Dixon, Illinois from 1983 to 2012, operator of the largest municipal fraud in U.S. history. In 2011, one of the city commissioners praised her "she looks after every tax dollar as if it were her own".

Crundwell began working in city hall in 1970 when she was a high school student. She became Dixon's comptroller and treasurer in 1983 and opened the curious RSCDA account in December 1990.

In the fall of 2011, Crundwell took 12 weeks of unpaid leave. Kathe Swanson, the city clerk, had to fill in for Crundwell and prepare the fiscal report for an upcoming council meeting.

Crundwell had never enabled the online option for the city's bank accounts, so Swanson couldn't view and print the statements. And the city's bank, Fifth Third Bank, hadn't mailed the statements.

Crundwell would advise Swanson to give only the last four digits of the pertinent accounts to email to the bank so it could fax the records to city hall.

"Swanson finally called the bank, and said, 'I want every statement of the City of Dixon's faxed to me in the next five minutes,' "

When she got the bank records, she saw three large deposits — of $200,000, $300,000 and $500,000 into an unknown account called "RSCDA — Reserve Fund" or Reserve Sewer Capital Development Account.

"My first thought was that Rita put a private account under the city's name because she was buying and selling horses and shielding the money from the IRS," Swanson says.

"That's when I really started looking at all the debits and credits, like gasoline and things like that. Well, the city has their own pumps, so I knew it wasn't a city account." Swanson says Dixon funds would first go into the Illinois Treasurer's Investment Pool [ITIP] state account in Springfield, the capital, because of better interest rates.

"We would get a fax from the state saying the money was in the account, whether it was from state sales tax, income tax, whatever," she says. "Once the money was in the ITIP account, Rita would call it up before 11 o'clock, and it would go into our capital development account — an honest account.

Then before she left for lunch, she'd go over to the capital development account book, write a check for 'treasurer,' payable to treasurer.

She'd take that check and bring it over to Fifth Third Bank in Dixon and deposit it into the RSCDA account, 'care of Rita Crundwell, Treasurer, City of Dixon.' "

Crundwell did this 169 times until she'd stolen $53.7 million.

She was fired in April **2012** after the discovery that she embezzled **$53.7 million** from the city of Dixon for over **22 years** to support her championship American Quarter Horse breeding operation. She was sentenced to nearly **twenty years** in prison and is scheduled to release on October 2029. However, Rita Crundwell has been released from federal prison in central Illinois on August 18, 2021 and taken to an undisclosed location.

As an Internal auditor what are the learnings from this important case?

Solution:

Complete absence of internal control, internal check and lack of ethical behavior:

Rita Crundwell first opened the fictitious account in 1990, she was also the only signatory to operate the account. Many banks, including Fifth Third, require additional people or entities to be involved so as to prevent fraudulent activities. A resolution is also required to open up an account at the bank. This resolution never took place.

Rita would make "fictitious" checks simply addressed to "treasurer" rather than under her name or the city's name and deposit them into the fictitious account. This is not usual behavior, and according to a former manager at Fifth Third, checks should have been addressed to "treasurer of the City of Dixon" or "City of Dixon."

You have learned the term "segregation of duties." In this case, Rita ' s bookkeeping duties should have been separated — by having someone other than Rita approve expenses as well as reconciling bank statements.

Crundwell also wrote lots of checks for large sums of money, which, acted as a clear red flag. It appears that the bank had proper procedures in place in theory but did not enforce them.

Aftermath of Fraud done by Rita

The city of Dixon, Illinois has dramatically changed many of its practices to ensure nobody has the extent of power Rita had to commit fraud for so long.

After she was dismissed, the city hired a new finance director who reorganized the city's finances and restructured the department. She implemented more internal controls so that no one person could complete an entire process by him- or herself including her. Today the city has hired more clerks that specialize in specific areas such as payroll and billing. Mail is no longer picked up by one person. Instead, it is delivered straight to City Hall.

https://harbert.auburn.edu/binaries/documents/center-for-ethical-organizational-cultures/cases/dixon-fraud.pdf

RISK MANAGEMENT

Meaning of Risk

Risk is a possibility that something bad will happen. Contract risk management minimises the probable loss through the effective and efficient management. It evaluates risks in terms of probability of occurrence and its impact. A simple example is given below.

Modern problem of using phone while driving: The impact of using phone while driving can range from none, to a near-miss, to collisions of various intensity which can result in injury or death to the driver, their companions, other road users and innocent bystanders, and damage to property.

Types of Risks

Systematic Risk: The overall impact of the market due to COVID, inflation, corruption, change in interest rate etc.

Unsystematic Risk: Asset-specific or company-specific uncertainty due to employee turnover, strike, higher cost of operations etc.

Political/Regulatory Risk: The impact of political decisions and changes in regulation.

Financial Risk: The capital structure of a company (degree of financial leverage or debt burden).

Country Risk: Uncertainties that are specific to a country.

Operational Risk: Uncertainty about a company's operations, including its supply chain and the delivery of its products or services.

Environmental Risk: Uncertainty about environmental liabilities or the impact of changes in the environment.

Management Risk: The impact that the decisions of a management team have on a company.

Legal Risk: Uncertainty related to lawsuits or the freedom to operate.

Competition: The degree of competition in an industry and the impact choices of competitors will have on a company.

Obsolescence Risk: In the rapid changing world, risk of obsolescence is high. Kodak Camera, Nokia, Tape-recorder are real life examples. Netflix renting of DVDs.

Definition of Enterprise risk management (ERM) as per COSO

Enterprise risk management (ERM) is *"the process of identifying and addressing methodically the potential events that represent risks to the achievement of strategic objectives, or to opportunities to gain competitive advantage".*

The fundamental elements of ERM are the assessment of significant risks and the implementation of suitable risk responses.

Risk responses include:

- **acceptance or tolerance of a risk;**
- **avoidance or termination of a risk;**
- **risk transfer or sharing** via insurance, a joint venture or other arrangement; and
- **reduction or mitigation of risk** via internal control procedures or other risk prevention activities.

Due to increased globalization of the economy, Covid 19 has created a havoc across the continents. Complete involvement on the part of board members and employees is essential in determining the risk appetite of a company, and in identifying and prioritising risks. Speed of onset and persistence of risks, in addition to impact and likelihood, are important considerations in the prioritisation of risks.

Continuous monitoring and concise reporting on key risk exposures are essential for effective risk management. Other important ERM concepts include: the risk philosophy or risk strategy, risk culture and risk appetite. These are expressions of the attitude to risk in the organisation, and of the amount of risk that the organisation is willing to take. These are important elements of governance responsibility.

A Risk Management Plan

A defined and documented process agreed upon by stakeholders for how risks will be identified, assessed, a decision made on mitigation (or if the risks will be accepted), how a response plan will be developed and what controls will be put in place to monitor risks.

Identify Risks: A way to efficiently capture identified various risks and add to the risk register.

Risk Register: A log of identified risks and their status. Risks are added to the register as they are identified and the impact and probability of occurrence are assessed through qualitative and quantitative methods.

Qualitative / Quantitative Analysis Tools: Methods for analysing / evaluating the probability and impact of risks on the organisation's objectives.

Response / Mitigation Plan: Determine if the risks are acceptable or not based on assessment and plan for mitigation.

Control Risks: Assess effectiveness through methods like risk audits and continually improve the project execution.

Risk Mitigation: The objective of risk mitigation is to reduce the probability and/or consequences of a risk event to an acceptable threshold and define appropriate response.

Questions To Ask:

- What are the available options?
- Tradeoffs (cost / benefit) of each option?
- Impacts of current decisions on options?

Risk mitigation actions may be costly and time consuming; Actions taken are balanced against priority level of the risk. Organisations typically transfer risk where possible, for example through product warranty or taking an insurance cover. Low-risk factors may be recognised by the Organisation but absorbed as a matter of policy.

Management responsibilities include:

- the risk architecture or infrastructure,
- documentation of procedures or,
- risk management protocols,
- training, monitoring and reporting on risks, and
- risk management activities.

Every entity exists to realise value for its stakeholders. Value is created, preserved, or eroded based on the management decisions in all activities right from setting strategy to operating the enterprise on day-to-day basis.

COSO Enterprise Risk Management (ERM)– Integrated Framework

The COSO Board released in September 2017 an update to the 2004 Enterprise Risk Management–Integrated Framework

The ERM Framework itself is a set of principles organized into five interrelated components:

1. **Governance and Culture**: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity. Tone at the top is a popular buzzword.
2. **Strategy and Objective-Setting**: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
3. **Performance:** Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritised by severity in the context of risk appetite. The organisation then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
4. **Review and Revision**: By reviewing entity performance, an organisation can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.
5. **Information, Communication, and Reporting**: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organisation.

Five Components Twenty Principles

Governance and Culture	Strategy and Objective-Setting	Performance	Review and Revision	Information, Communication, and Reporting
1. Exercise Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops, and Retains Capable Individuals	6. Analyses Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View	15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues Improvement in Enterprise Risk Management	18. Leverages Information and Technology 19. Communications Risk Information 20. Reports on Risk, Culture, and Performance

RECOMMEND CONTROLS TO PREVENT AND DETECT FRAUD AND EDUCATE TO IMPROVE THE ORGANIZATION'S FRAUD AWARENESS

There are several controls that an organization can implement to prevent and detect fraud, and education is a crucial component in improving an organization's fraud awareness.Here are some recommendations for controls and educating across the entity:

1. **Segregation of duties:** Ensure that no single person has control over multiple aspects of a process or transaction. For example, the person who approves a purchase should not be the same person who pays for it. Maker, Checker and Approver is an excellent tool to prevent errors and frauds.
2. **Rotation of duties**: Ensure that there is periodical rotation of duties for key positions. We saw in the largest municipal fraud that in the absence of rotation of duties, huge fraud perpetrated by one employee gone unnoticed. Punjab National Bank fraud also happened due to absence of mandatory job rotation or transfer of few employees of the branch.
3. **Mandatory vacation:** Having a HR policy for giving mandatory vacation to key employees helps the employees to come fresh after vacation and also prevents employees from hiding their tracks of crime.
4. **Treat employees well**. It has been observed that if the employees are treated well by giving timely rewards and recognition for their work, they feel motivated. If they are treated badly like being underpaid or overlooked for promotion, they look for the opportunity and rationalise to do frauds to take revenge on their employers.
5. **Regular audits**: Conduct regular internal audits especially at remote locations where there are significant projects being executed or manufacturing facilities are run to identify potential fraud and ensure compliance with internal controls.
6. **Background checks**: Conduct thorough background checks on employees, especially those in positions of trust or responsibility.
7. **Whistleblower hotline:** Implement a confidential hotline for employees to report suspicious activity without fear of retaliation.
8. **Use of technology:** Implement fraud detection software and use data analytics to identify patterns of suspicious activity.
9. **Fraud awareness training:** Provide periodical training to all employees on the types of fraud that can occur, how to identify it, and how to report it. Also ensure that adequate documents are kept in HR as evidence to prove that the employee participated in the training and understood it. This will help on a later date if the fraudulent employee feigns ignorance.
10. **Code of conduct:** Establish a code of conduct that clearly defines ethical behavior and expectations for employees.
11. **Management oversight and Tone at the top:** Ensure that management regularly reviews and approves transactions and financial statements. Ensure that independent directors are really independent.
12. **Reinforce accountability:** Hold employees accountable for their actions and ensure that consequences are enforced when necessary.
13. **Document retention:** Establish policies for the retention and destruction of records to ensure that important documents are not lost or destroyed.

Communicate all key changes to Policies and Procedures of the entity to all stakeholders like employees, vendors, customers and document evidence in support of the same that these stakeholders have read and understood the implications of changes made.

By implementing the above controls and providing education on fraud prevention and detection, organizations can help protect themselves against potential fraud and improve their overall fraud awareness.

ROLE OF INTERNAL CONTROL IN THE NEW DIGITAL ERA

Robotic Process Automation (RPA)

Companies across industries are working to digitize parts of the business with robotic process automation (RPA), often referred to as "bots." RPA involves the use of software robots to automate routine, repetitive, and rules-based tasks that were previously performed by humans. By automating these tasks, RPA can reduce errors, increase efficiency, and improve the accuracy and timeliness of data.

RPA bots are programmed to perform tasks in a consistent manner, which reduces the risk of errors and inconsistencies in data. By automating processes, RPA can also reduce the risk of human error.

RPA can provide an audit trail of all activities performed by the bots. This means that auditors can easily track and verify activities, which can improve the accuracy of financial statements and reduce the risk of fraud.

Enhanced monitoring and reporting: RPA can provide real-time monitoring and reporting of activities, which can help identify and address potential issues quickly. This can be particularly valuable in areas such as compliance, where organizations need to demonstrate adherence to regulations and policies.

Reduced operational risks: RPA can help reduce operational risks by automating tasks that are susceptible to errors or require significant manual effort. This can lead to more efficient processes and lower operational costs.

However, it's important to note that while RPA can enhance internal controls, it's not a substitute for a strong internal control system. Organisations still need to establish and maintain effective internal controls that are aligned with their business objectives and risks. Additionally, RPA implementation should be carefully planned and monitored to ensure that it is working effectively and in compliance with relevant regulations and policies.

Artificial Intelligence and Machine Learning

Artificial intelligence (AI) and machine learning (ML) are revolutionising various industries, including the field of internal control. Internal control refers to the processes, procedures, and systems that an organization has in place to ensure that it operates efficiently, effectively, and ethically.

AI and ML can enhance internal control by automating repetitive and time-consuming tasks, providing insights into patterns and anomalies, and reducing the risk of fraud and errors. Here are a few examples of how AI and ML can improve internal control:

Fraud detection: AI and ML algorithms can analyse large amounts of data to detect patterns that may indicate fraud. These algorithms can also learn from historical data to identify new patterns and adapt to changing fraud tactics.

Risk assessment: AI and ML can be used to identify and assess potential risks, such as cybersecurity threats or compliance violations. By analysing data from various sources, these technologies can provide a more comprehensive and accurate risk assessment.

Process automation: AI and ML can automate routine processes, such as data entry or invoice processing, reducing the risk of human error and freeing up time for internal control professionals to focus on higher-value tasks.

Predictive analytics: By analysing historical data and identifying outliers, AI and ML can predict future trends and patterns, helping organizations make informed decisions about internal control measures and resource allocation.

However, it is important to note that AI and ML are not a replacement for human expertise and judgment. These technologies should be used in conjunction with internal control professionals to ensure that the insights they provide are accurate and relevant.

Additionally, organisations must be mindful of ethical considerations, such as bias and privacy, when implementing AI and ML in their internal control processes.

Blockchain Technology

Blockchain is a digital ledger technology that is used to store data in a secure and decentralised way. It offers numerous benefits for internal control in various industries. One of the key benefits of blockchain for internal control is its ability to provide an immutable record of transactions. This means that once data is recorded on the blockchain, it cannot be altered or deleted without the consensus of the network participants. This feature ensures that the data is trustworthy and tamper-proof, which is critical for maintaining a strong internal control environment.

Another benefit of blockchain for internal control is its ability to provide transparency and accountability. Since all transactions are recorded on a shared ledger, all network participants have access to the same information. This makes it easier to identify discrepancies, detect errors, and investigate fraud.

Furthermore, blockchain can automate various internal control processes, such as transaction approvals, reconciliation, and audit trails. Smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code, can be used to automate these processes, ensuring accuracy and consistency.

In summary, blockchain can improve internal control in a number of ways, including providing a secure and tamper-proof record of transactions, enhancing transparency and accountability, and automating internal control processes. As a result, blockchain is increasingly being adopted by businesses across various industries to strengthen their internal control environment.

Cloud Computing

Cloud computing is a technology that allows users to access computing resources, such as servers, storage, applications, and services, over the internet. Internal control, on the other hand, is a process designed to provide reasonable assurance regarding the achievement of an organization's objectives in terms of effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

When it comes to cloud computing, internal control is essential to ensure that the organization's data, systems, and processes are secure and reliable. Here are some ways internal control can be implemented in the context of cloud computing:

Risk assessment: The organisation should conduct a risk assessment to identify potential risks associated with using cloud computing services, such as data breaches, system failures, and vendor lock-in.

Vendor selection: The organisation should select cloud computing vendors that meet its security and compliance requirements. This may include evaluating vendors' security controls, certifications, and audit reports.

Service level agreements (SLAs): The organisation should negotiate SLAs with cloud computing vendors that define the level of service, performance, and availability that is required. The SLAs should also include provisions for data privacy, security, and compliance.

Access controls: The organisation should implement access controls to ensure that only authorized personnel can access its cloud computing resources. This may include using multi-factor authentication (MFA), role-based access control, and encryption.

Data encryption: The organisation should encrypt data before storing it in the cloud, to prevent unauthorized access and data breaches.

Monitoring and reporting: The organisation should implement monitoring and reporting mechanisms to detect and report security incidents and data breaches. This may include using intrusion detection systems, log monitoring, and vulnerability scanning.

Overall, internal control is critical to the effective and secure use of cloud computing services, and should be an integral part of an organisation's cloud computing strategy.

PRACTICE QUESTIONS

1. **While planning an audit, the auditor does not think that it would be necessary to understand internal controls. Advise the auditor in this regard.**

   Solution: The auditor shall obtain an understanding of internal control relevant to the audit. Although most controls relevant to the audit are likely to relate to financial reporting, not all controls that relate to financial reporting are relevant to the audit. It is a matter of the auditor's professional judgment whether a control, individually or in combination with others, is relevant to the audit.

2. **The team member of the auditor was of the view that understanding the internal control of the company would not help them in any manner in relation to audit procedures to be applied while conducting the audit.**

   Solution: The view of the team member of the auditor is incorrect because understanding the internal control of the company would help the auditor and his team members in designing the nature, timing and extent of audit procedures to be applied while conducting the audit of the company.

3. **One of the team members of the auditors was of the view that risks that were identified during the course of audit were not required to be documented. Explain with a reason whether the viewpoint is justified.**

   Solution: The auditor shall document the identified and assessed risks of material misstatement at the financial statement level and at the assertion level; and the risks identified, and related controls about which the auditor has obtained an understanding. Keeping in view the above, the viewpoint is not justified because risks that were identified during the course of audit were required to be documented by the auditors.

4. **One of the directors of the Company was of the view that internal financial controls have nothing to do with accounting records of a company. Comment.**

   Solution: The meaning of internal financial controls as, "the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information." In view of above, viewpoint of director is incorrect.

5. **The office manager controlled the company's financial operations. She did payroll, accounts payable, invoicing and cash receipts. She rarely took time off, and even then, came back when they needed to run checks or payroll. The owner viewed her as key to running the business. What are your recommendations as an internal auditor of the organizations in view of evaluating Internal Control?**

   Solution:

   - Segregation of duties is critical so that everything isn't done by one person. Having one person do everything can lead to fraud and theft. Oversight can help, but segregation of duties is the best alternative.
   - Take the three primary cash responsibilities such as accounts payable, accounts receivable, and payroll. Cross train others so that they can take over if needed.
   - Provide close oversight of cash operations.

CASE STUDY

1. Credit Suisse Crisis

Background

The second largest 167-year-old Swiss bank, Credit Suisse was bailed out by UBS (Union Bank of Switzerland- one of the predecessor firms' name), the biggest number one Swiss Bank by doing a buy out and the AT1 bonds of Credit Suisse Bank worth 17 BN $ were completely written off.

A bailout is when an individual, business, or organization provides capital or other resources to a failing company to prevent it from collapsing.

UBS agreed to buy rival bank Credit Suisse for 3 billion Swiss francs ($3.23 billion) and assume up to $5.4 billion in losses, in a shotgun merger planned by Swiss authorities. Under the deal, on the orders of the Swiss regulator, 16 billion Swiss francs ($17 billion) of Credit Suisse's Additional Tier 1 debt will be written down to zero.

Credit Suisse had made a few questionable acquisitions and had been penalized many times, the reputation of the bank was in question leading to a tremendous slowdown in all its businesses, and on 3-year average business growth for most of its segment was negative over 10% YoY.

Due to negative sentiment about Credit Suisse bank, by December 2022 just in a couple of months, huge deposits of over 150 billion were withdrawn from the bank.

The problem faced by Credit Suisse bank was different as compared to Silicon Valley Bank (SVB) which had an ALM mismatch. In the case of Credit Suisse, there were changes in the top management many times. This had put a lot of liquidity pressure on the bank & news of the SVB crisis led to another panic situation triggering further liquidity crisis for the Bank.

The collapse of Credit Suisse could impact Switzerland's reputation as a stable, strong country for banking.

Reasons for downfall of Credit Suisse

In 2021, the collapse of the U.S. family investment fund Archegos Capital and British finance firm Greensill Capital triggered a pre-tax loss of close to $1 billion for Credit Suisse Bank.

Following the collapse of Archegos, Credit Suisse's investment bank CEO and chief risk and compliance officer left the company. An independent investigation of Credit Suisse's role in the Archegos scandal found that the bank had failed to "effectively manage risk," but suggested that no fraudulent or illegal conduct occurred.

Chairman Antonio Horta-Osorio resigned in January 2022 from the company as he broke COVID-19 quarantine regulations. Rumor is circulated that Credit Suisse Bank faces impending failure, prompting clients to pull about $119 billion in funds in the last quarter of the year. Credit Suisse in March 2023 said it will borrow up to $54 billion from the Swiss National Bank. U.S. institutions Silicon Valley Bank and Signature Bank failed, setting the global financial system on edge.

Material Weaknesses in Financial controls over financial reporting and risk assessments

In its Annual Report 2022 Credit Suisse Bank management admitted "material weaknesses" in its internal controls over financial reporting and risk assessments in 2022 and 2021. "As of December 31, 2022, the Group's internal control over financial reporting was not effective, and for the same reasons, management has reassessed and has reached the same conclusion regarding December 31, 2021."

Credit Suisse's 'material weaknesses' mainly related to the failure to design and maintain effective risk assessments; and this problem has been vastly seen in its financial statements.

Credit Suisse also failed to design and maintain effective monitoring activities relating to management oversight, resource allocation, and deficiency assessment. This lack of oversight and monitoring made it difficult for the bank to identify and address issues before they become major problems.

Controls over consolidated statements of cash flows were inadequate

Finally, Credit Suisse's material weakness disclosure revealed that their controls over the classification and presentation of the consolidated statement of cash flows were inadequate. This resulted in revisions to their previously issued financial statements,

Auditor PricewaterhouseCoopers (PwC) in their report included an "adverse opinion" on the effectiveness of the bank's internal controls over its reporting, but its financial statements "present fairly, in all material respects" the financial position of the bank in 2020 through 2022.

2. Silicon Valley Bank Collapse

Background

Silicon Valley Bank (SVB) was founded in the year 1983 at Silicon Valley, California. It was the 16th largest U.S. bank before its collapse. SVB specialized in financing and banking for venture capital-backed startup companies -- mostly technology companies. Venture capital firms did business there as well as several tech executives. SVB had assets totaling $209 billion at the end of 2022, according to the Federal Deposit Insurance Corporation (FDIC).

The Silicon Valley Bank (SVB) failure is the largest bank failure since 2008.It's been a long time since the last failure that was as big as this one, which was Washington Mutual.

Reasons for collapse of Silicon Valley Bank

Many of SVB's customers were tech startups and hence a concentration of money from just one sector. Due to rising inflation rates and other things, many companies started struggling to get additional financing from venture capital and elsewhere. So, they needed to withdraw their deposits at SVB. When one industry suddenly needed cash, many companies went to the bank and tried to withdraw all their money. That's a run on the bank.

A bank doesn't have all that cash on hand. SVB, had invested that money. When these tech startups wanted all their money in cash it resulted in a run on the bank. SVB had invested it in low-yield treasury bonds that would pay interest. But given the rate of inflation — the interest rate was under 2%, very low — the bonds were worth more if they were held for a long time.

But the Bank had to sell them quickly and at a loss. So, what happened was it incurred a huge loss. As a result, Bank management tried to raise more money by issuing their own bonds on the open market.

Lack of diversification

Silicon Valley Bank invested a large amount of bank deposits in long-term U.S. treasuries and agency mortgage-backed securities. However, bonds and treasury values fall when interest rates increase.

When the Federal Reserve hiked interest rates in 2022 to combat inflation, SVB's bond portfolio started to drop. SVB would have recovered its capital if they held those bonds until their maturity date.

SVB used to lend out money in short durations. However, in 2021, they shifted to long-term securities such as treasuries for more yield, and they did not protect their liabilities with short-term investments for quick liquidations. They were insolvent for months because they could not liquidate their assets without a large loss.

SVB didn't have the cash on hand to liquidate the deposits as they were tied up in long-term investments. They started selling their bonds at a significant loss, which caused distress to customers and investors.

Within 48 hours after disclosing the sale of assets, the bank collapsed.

California Department of Financial Protection & Innovation appointed the Federal Deposit Insurance Corporation (FDIC) as receiver. California regulators shut the bank down on March 10, 2023.

Unlike personal banking, SVB's clients had much larger accounts. It didn't take long for money to diminish during the bank run, with the escalating pace of withdrawals causing a snowball effect. Most customers had deposits more than the $250,000 FDIC limit.

SVB stockholders and investors took a big hit because, unlike customers, they were not backed by FDIC on their investment. Large tech companies with significant cash in SVB include Etsy, Roblox, Rocket Labs and Roku.

SVB purchased by First Citizens Bank

On March 26, 2023, FDIC announced First Citizens Bank will purchase Silicon Valley Bank and assume the majority of its deposits and loans. As of March 10, Silicon Valley Bank reported nearly $167 billion in total assets and $199 billion in deposits.

First Citizens Bank will purchase about $72 billion in assets at a discounted rate of $16.5 billion. FDIC will remain in control of nearly $90 billion in assets and securities in its receivership. All 17 of Silicon Valley Bank's branches will operate under Silicon Valley Bank, a division of First Citizens Bank.

The FDIC also estimated that the SVB failure cost nearly $20 billion.

Mismatch of ALM – Major reason

One of the key issues with SVB was the ALM (asset-liability management) mismatch, where they invested short-term funds into long-term securities.

The bank had made an ill-informed and reckless bet that the Fed would keep interest rates low and thus, when the Fed hiked aggressively SVB's unrealized bond losses soared. Interest rates and bonds have an inverse relationship which means as interest rates rose, bond prices fell, resulting in the massive loss-making bond portfolio.

One of the major rating's agencies, Moody's, subsequently downgraded SVB' credit rating. In response to downgrading, SVB announced its intention to raise $2.25 billion in fresh capital by selling new shares, which didn't go down well with the market. The sheer size of SVB's illiquid 'held-to-maturity' investments (poorly performing bond portfolio) spooked depositors who realized it would be near impossible to liquidate the sizeable holdings into cash to meet withdrawals in the event of a run on the bank.

SVB had inadequate risk management and internal controls that struggled to keep pace with its growth,

SVB's failure brought with it the demise of Signature Bank – a favourite banking institution for the crypto industry – and Silvergate Bank.

LESSON ROUND-UP

- As per Section 134 of the Companies Act, 2013, the term "Internal Financial Controls" means the policies and procedures adopted by the company for ensuring, orderly and efficient conduct of business, including adherence to company's policies, safeguarding of its assets, prevention and detection of frauds and errors, accuracy and completeness of the accounting records, and timely preparation of reliable financial information.
- Objectives and various Dimension of Internal Control.
- Difference between Internal check and Internal Control.
- Types of Control – Preventive, Detective, Input , Output.
- Benefits and Limitation of Internal Control.
- Internal Control Techniques such as Segregation of duties, Access Control, Auditing, Risk Management.
- Internal Control Frameworks (COSO, CADBURY).
- Implementation of internal controls: Internal auditors play a critical role in the implementation of internal controls. They provide assurance that internal controls are designed and operating effectively, and help identify areas where improvements can be made.
- Role of Internal Control in the New Digital Era such as:
  - (i) Robotic Process Automation (RPA)
  - (ii) Artificial Intelligence
  - (iii) Block chain Technology
  - (iv) Cloud Computing.

TEST YOURSELF

(*These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation*)

MCQs Based Questions

1. Internal check is meant for:
   - (a) Prevention of frauds
   - (b) Detection of frauds
   - (c) Helping audit in depth
   - (d) Detection of errors.

   Answer: (c) Helping audit in depth.
2. Internal controls and internal check are:
   - (a) One and the same
   - (b) Different
   - (c) Internal control includes internal check
   - (d) None of the above.

   Answer: (c) Internal control includes internal check

3. In comparison to the independent auditor an internal auditor is more likely to be concerned with –
   (a) Cost accountancy system
   (b) Internal control system
   (c) Legal compliance
   (d) Accounting system.

   Answer: (b) Internal control system.

4. Which of the following is responsible for establishing a private company's internal control?
   (a) Management
   (b) Auditors
   (c) Management and auditors
   (d) Committee of Sponsoring Organizations.

   Answer: (a) Management.

5. Internal controls can never be considered as absolutely effective because:
   (a) their effectiveness is limited by the competency and dependability of employees
   (b) not all organizations have internal audit departments
   (c) controls are designed to prevent and detect only material misstatements
   (d) Internal controls prevent separation of duties.

   Answer: (a) their effectiveness is limited by the competency and dependability of employees.

6. An act of two or more employees to steal assets or misstate records is frequently referred to as:
   (a) collusion
   (b) material weakness
   (c) control deficiency
   (d) Significant deficiency.

   Answer: (a) Collusion.

7. The process of ensuring no single employee is in control of receiving, recording, and authorizing a transaction is known as _____.
   (a) authorization
   (b) segregation of duties
   (c) accuracy
   (d) completeness.

   Answer: (b) segregation of duties.

8. Due to inherent limitations of internal control system it can provide _____ assurance that its objectives are achieved.
   (a) Reasonable

(b) Absolute

(c) Negative

(d) All of these.

Answer: (a) Reasonable.

9. A Graphic presentation of internal controls in the organisation and is normally drawn up to show the controls in each section or subsection is known as:

(a) Narrative Records

(b) Check List

(c) Internal Control Questionnaire

(d) Flowchart.

Answer: (d) Flowchart.

10. Internal check is a check on _____ transactions whereby work carried out by one person is checked by _____.

(a) Unusual; auditor

(b) Unusual; another

(c) Day-to-day; auditor

(d) Day-to-day; another.

Answer: (d) Day-to-day; another.

11. When more persuasive audit evidence is needed regarding the effectiveness of a control:

(a) It may be appropriate to increase the extent of testing of the control and reduce the extent of the degree of reliance on controls

(b) It may be appropriate to decrease the extent of testing of the control as well as the degree of reliance on controls

(c) It may be appropriate to decrease the extent of testing of the control and increase the extent of the degree of reliance on controls

(d) It may be appropriate to increase the extent of testing of the control as well as the degree of reliance on controls.

Answer: (d) It may be appropriate to increase the extent of testing of the control as well as the degree of reliance on controls.

12. The objective of internal audit is:

(a) To prevent errors and frauds

(b) To detect errors and frauds

(c) To improve financial controls

(d) All of the above.

Answer: (d) All of the above.

Practical Questions:

1. "The auditor shall obtain an understanding of the major activities that the entity uses to monitor internal control over financial reporting" Explain.
2. Obtaining an understanding of the entity and its environment, including the entity's internal control, is a continuous, dynamic process of gathering, updating and analysing information throughout the audit. Analyse and explain giving examples.
3. What are the limitations of Internal Control?
4. What are the benefits of Internal Control?
5. Explain the role of Internal Auditor in implementing the effective Internal Control System.
6. What are the various types of control that are required in every organisation?
7. What do you mean by COSO Internal Control Framework? Explain its various components and Principles.
8. Explain what do you mean by the term Enterprise Risk Management? What are the various components and principles prescribed in COSO Enterprise Risk Management Integrated Framework?
9. Internal control role in this digital era of RPA, Blockchain, Artificial Intelligence and Machine learning and Cloud computing.

Case Study

Sam and his brother Bob owners and operators of tractors for 30 years as a closely held business. A local bank was financing them based on the inventory of tractors worth millions of Rupees. Their wives were sharing the accounting duties.

Both wives of the brothers retired from business because of their age. James son of Sam who was a graduate was appointed as the accountant. Earlier, James would approve vendor invoices, Julie will prepare cheques which will be signed by either of brothers.

The brothers entrusted with Sam all aspects of bookkeeping, accounts payable, accounts receivable, payroll and accounts reconciliations. Later on they also gave him cheques signing authority and credit card in the name of the company.

James got married and his personal expenses increased and he soon found it difficult to maintain the life style he had known when he was a bachelor and living with his parents.

Having been under financial pressure, he looked for the opportunities to make extra money from the company. He used the company funds and started manipulating the books of account to hide his crime for maintaining his life style. The brothers initially had attributed the cash flow problem to a downturn in the economy. But later on wanted to know why there is a regular cash crunch in the business even after economy was slowly improving.

One of James cousin, Daniel a CA with more than 5 years of experience was appointed to do an internal audit on behalf of the owners discovered the fraud, when he was going through the bank statements. Several cheques were issued by James to himself on a regular basis. When confronted, James confessed to the crime of embezzling thousands of rupees.

You are required to submit a detailed internal audit report on various aspects of the case based on the concepts given in this study lesson and give appropriate recommendations to the owners.

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's

- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022