

Audit, Business Processes and Digitalization [BL 5]

Business Level II | CA Sri Lanka

Study Text

By: M B G Wimalarathna [FCA, FCMA, FMAAT, MCIM, CPFA, CIPFA, MCPM] [MBA (PIM/USJ)]

Contents of the Curriculum

PART A: INTRODUCTION TO CORPORATE GOVERNANCE, RISKS AND CONTROLS

- A.1: Corporate Governance
- A.2: Internal Controls

PART B: BUSINESS PROCESSES AND INTERNAL CONTROLS

- B.1: Sales Management
- B.2: Procurement Cycle Management
- B.3: Payroll Management
- B.4: Cash Management
- B.5: Property, Plant & Equipment Management
- B.6: Inventory Management

PART C: DIGITALIZATION AND BUSINESS PROCESSES

- C.1: Effectiveness of Controls and Digitalization

PART D: ETHICS AND VALUES

- D.1: Introduction to Assurance Engagements
- D.2: Ethics and Agreeing the terms of the Engagement

PART E: FUNDAMENTALS OF AUDIT AND ASSURANCE

- E.1: Risk Assessments
- E.2: Audit Planning and Documentations
- E.3: Audit Procedures and Audit Evidence
- E.4: Audit Finalization and Reporting

PART A: INTRODUCTION TO CORPORATE GOVERNANCE, RISKS AND CONTROLS

A.2: Internal Controls

Internal controls [internal control system] are the policies & procedures established and practiced by an organization mainly to protect its resources as well as secure business continuity for a long period

Notes:

Chapter contents

- A.2.1. Definition of internal control
- A.2.2. The elements of an internal control system
- A.2.3. Internal controls
- A.2.4. Financial, operational and compliance controls
- A.2.5. Preventive, detective and corrective controls
- A.2.6. Control procedures
- A.2.7. Internal control risks
- A.2.8. Information and communication in internal control
- A.2.9. Information processing controls
- A.2.10. Monitoring an internal control system
- A.2.11. Limitations of an internal control system
- A.2.12. Governance and risk

A.2.1. Definition of internal control

An internal control system (IC system) consists of processes to provide reasonable assurance about the achievement of the organization's objectives with regard to efficiency and effectiveness of operations, reliability of financial reporting and compliance with laws and regulations

A definition based on the Committee of Sponsoring Organizations (COSO) internal control framework, an internationally-recognized authority on risk management and internal control, defines an internal control system as:

- Processes put into effect by the board of directors and management
- That are designed to provide reasonable assurance regarding the achievement of objectives in the following areas:
 - ✓ Effectiveness and efficiency of operations
 - ✓ Reliability of financial reporting
 - ✓ Compliance with laws and regulations

Internal control is concerned with risks that an organization faces. It reduces risks at the level of business processes and operations

A.2.2. The elements of an internal control system

The components of an IC system are a control environment, risk assessment, information and communication, internal controls and monitoring of the effectiveness of controls of the IC system

The COSO internal control system framework has five components:

- A control environment.** This refers to the culture of the organization and its attitudes to risks. A risk-awareness culture is created by the leaders of the organization, who should provide an example to all other employees. The effectiveness of an internal control system depends on the attitudes to risk and risk awareness of the people in it.
- Risk assessment.** This requires management to consider the impact of possible changes in the internal and external environment and to potentially take action to manage the impact. Risk assessment should take account of the probability of a change occurring as well as the potential impact.
- Control activities.** These are the internal controls, which are designed to fulfil a particular control objective.
- Information and communication.** Internal control systems require processes and procedures for the communication of information to relevant people about risks and controls.
- Monitoring.** There should be a process for regular monitoring of the effectiveness of the internal controls and other components in the internal control system

A.2.3. Internal controls

An internal control system is made up of many different internal controls. Each control has a particular purpose or 'control objective'

Key features of internal controls

- ✓ Internal controls may exist within a particular function (department) or within a particular activity.
- ✓ Each control has a particular purpose or 'control objective'.

- ✓ Internal controls may apply to business operations, financial reporting or compliance with laws and regulations.
- ✓ Controls may be designed to prevent an operational failure, detect a failure when it occurs or correct a failure that has occurred.
- ✓ There is a risk that internal controls may fail. The risk of a failure in an internal control is known as 'internal control risk'

A.2.4. Financial, operational and compliance controls

Internal controls are designed and implemented to reduce risks. They may be described as operational controls, financial controls and compliance controls. Alternatively, they may be described as preventive, detective and corrective controls

Internal controls can be classified in several different ways. One method is to classify internal controls as financial controls (or financial reporting controls), operational controls and compliance controls

Financial controls

Financial internal controls should, taken together, reduce the risks of errors or fraud in accounting systems and financial reporting

Errors or fraud could result in losses for the organization, as well as incorrect financial statements. Weak controls may also mean that financial assets, such as cash, are not properly safeguarded

Examples of financial controls are shown in the following tables

Risk	Controls
Failure to protect cash receipts	All receipts of cash must be recorded immediately
Objective of control To ensure that cash receipts are protected and none is stolen	Cash should be transferred to a safe location (for example, a safe) by an authorized person
	There should be regular reconciliations between actual cash held and records of cash receipts
In a supermarket, for example, receipts of cash are recorded at the check-out desk. Cash is transferred regularly from check-out desks to a safe in the store. Regular reconciliations of actual cash and cash receipts are made	

Risk	Controls
Employees claim more money in expenses than they are entitled to	An employee must submit a formal claim for expenses to a specified person. These should be supported by supporting documents as evidence of the spending

Objective of control To ensure that employees are paid only for genuine expense claims	The specified person should check the claim and (if it is correct in detail and the claims are for valid items of expense) should authorize it for payment (by signing the claim form)
	The authorized claim is submitted to the accounts department for payment. The claim form is checked to make sure that the signature of the authorizing person is genuine. The payment is recorded and the claim form is kept on file

Operational controls

Operational controls are controls that reduce the risk of a loss of efficiency or effectiveness in business operations

Risk	Controls
The company's delivery vehicles will break down while making deliveries to customers	Delivery vehicles should be given a maintenance inspection at regular intervals. There should be an operational schedule for maintenance of each vehicle
Objective of control To reduce the risk of breakdown	A list of items to check is provided for maintenance inspections
	The maintenance engineer should make all the checks in the list and record the fact that the check has been made
There should also be controls to ensure that, if faults are found in a maintenance check, corrective measures are taken	

Risk	Controls
Unauthorized individuals may gain access to a building	All visitors are met by a receptionist. The receptionist puts a call through to the person that the visitor is meeting. The visitor is asked to sign in a visitors book. The visitor is given an identity badge and asked to wear it. Security guards are employed to watch for visitors who avoid the receptionist. They allow entry only to visitors showing a visitor badge. CCTV cameras are used to monitor the movement of individuals through the building. All side doors to the building are kept locked and may be opened only by authorized personnel with keys
Objective of control To prevent unauthorized access to the building	

Compliance controls

Compliance controls are implemented to reduce the risk of failure to comply with laws or regulations. The nature of controls varies with the nature of the law or regulation. For example, controls to ensure compliance with food hygiene regulations will be different from controls in banks to comply with anti-money laundering regulations

A.2.5. Preventive, detective and corrective controls

Preventive controls

Preventive controls are controls that are designed to prevent operational errors from happening in the first place. Some examples of preventive controls are as follows

Preventive controls	Purpose
Use of identity codes and passwords in an IT system	To prevent unauthorized access to the system
Checking invoices received from suppliers against goods received notes showing details of goods actually received	To prevent payment to suppliers for goods that have not been received
Supervision of employees at work	To prevent time wasting or inefficient working by employees

Detective controls

Detective controls are controls that are designed to detect errors once they have happened

Detective controls	Purpose
Carrying out a bank reconciliation, to make sure that the accounting records for cash agree with a statement from the bank	To detect any errors in the accounting records for cash
Counting physical inventory in store and comparing actual quantities counted with the quantities shown in the inventory records	To detect either (1) errors in the inventory records or (2) unexplained losses of inventory
Providing management with regular reports comparing budgeted performance with actual performance during a given time period	To prevent time wasting or inefficient working by employees

Corrective controls

Corrective controls are controls that are designed to minimize or negate the effect of errors or risk events. Examples of corrective controls are as follows

Corrective controls	Purpose
Backing up a computer at the end of each day and storing the back up at a remote location	To minimize the loss of data in the event of computer system failure and loss of data
Procedure to ensure that the latest valid backup can be adequately and quickly restored	To minimize downtime during a restore from backup

A.2.6. Control procedures

There are different types of control process or procedure. One approach to categorization of internal control procedures is the mnemonic SPAMSOAP

Internal control procedures are similar for financial, operational and compliance controls

- Segregation of duties
- Physical
- Authorization and approval
- Management
- Supervision
- Organization
- Arithmetical and accounting
- Personnel

Segregation of duties	Duties should be separated between two or more people. This means that the same person is unable to perform two key tasks, and also that one person acts as a check on what another person has done. For example, the person authorizing an item of expenditure should not be the same person who makes the payment
Physical controls	These are measures that act as physical protection for an asset, such as a security guard, a lock on a door, and swipe cards for entry to a room or building. Another type of physical control is a check to make sure of the actual existence of an asset. The accounting records may show that an organization owns certain assets, such as equipment or inventory. A physical control would be a regular check to make sure that assets exist, as shown in the accounting records
Authorization and approval controls	All transactions should require authorization or approval by an appropriate responsible person. Authorization limits should be specified; for example, managers at a certain level in the organization should not authorize spending above Rs. 20,000
Management controls	Managers provide control through analysis and review of performance

Supervision controls	Supervision of day-to-day activities by employees in a work group should help to ensure that all the employees do their work correctly and efficiently
Organization controls	Controls are provided by organization structures, such as lines of reporting, lines of authority, authority and responsibility for managers in each position in the organization
Arithmetical and accounting controls	To check the correct and accurate recording and processing of transactions; for example, reconciliations and trial balances. An example is the reconciliation performed between the fixed asset register and the fixed asset values recorded in the accounts
Personnel controls	Attention should be given to selection, training and qualifications of personnel, as well as personal qualities. The quality of any system is dependent on the competence and integrity of those who carry out control operations

A.2.7. Internal control risks

Internal control risks are risks that internal controls will fail to achieve their intended control objective. Reasons for control failure include poor design of the controls, overriding of controls by management or collusion between fraudsters

Internal control risks are risks that internal controls will fail to achieve their intended purpose. They are another category of operational risks

Reasons to internal controls unable to achieve intended objectives

They may be designed badly	As a result they are unable to perform their intended function properly	For example, management may receive control reports about operational or financial performance every six months. Receiving reports after six months is too late for managers to take control action at the best time. The management control is badly designed: reports should be more frequent
Employees are unaware of the control	As a result, the control is not implemented	It is essential to communicate information about controls to all relevant personnel
The control may be ignored in practice and not applied	If a control is ignored, it cannot be effective	An example is 'management override' of a control. Management ignores the control for their own actions, taking the view that the

		control applies to everyone else, but not to themselves
Controls are deliberately avoided	Someone committing fraud will look for ways to avoid controls and may do this through collusion with someone else	An example is collusion between two people, where one is supposed to check the work of the other (segregation of duties). By working ('colluding') together, two people may be able to negate a control
Human error	Controls may be applied incorrectly, or employees may make mistakes	

CASE STUDY

A well-publicized example in the UK of a failure in internal control was the appointment in 2010 of a new chairman of Co-operative Bank, a bank with ambitions for major expansion. The individual had no previous experience in banking and did not even know the value of the bank's assets. He resigned in 2011, but it soon became apparent that the bank had incurred major losses as a result of a merger. The bank was rescued from imminent collapse in 2013 by a consortium of hedge funds that owned bonds of the bank.

When it was reported in 2013 that this ex-chairman had been filmed buying drugs illegally during his period as chairman, the question of his original appointment was raised in the UK media.

- How was a person without any previous experience in banking made chairman of a large and ambitious bank?
- Appointments of bank chairmen must be approved by the UK banking regulator. Why did the banking regulator approve the appointment of someone who knew little or nothing about banking?

This case illustrates the potential consequences in failures in personnel controls, both in the bank itself and also by the banking regulator

A.2.8. Information and communication in internal control

An effective IC system requires that information about risks and controls should be communicated to the relevant people in a timely fashion

Information about operational risks and controls should be communicated to the people who are responsible for applying the controls. The communication system should be capable of communicating top-down, bottom-up and across the organization as a whole

Information technology systems make this communication much easier, with email, intranet, electronic noticeboards, as well as online systems that can be used to document risks and associated controls which are accessible to employees across the business

This aspect of an internal control system is concerned with ensuring that individuals are:

- Aware of what is expected from them
- Provided with sufficient detail on time to enable them to perform their control tasks effectively

Whistle-blowing

There is a risk in many organizations that one or more individuals will behave improperly, possibly committing fraud or another crime, such as accepting a bribe from a supplier in return for placing a purchase contract with the supplier. Colleagues may be aware of the wrongdoing, but afraid to report it to a senior manager

Companies may establish a whistle-blowing system that enables employees to report wrongdoing by colleagues or managers in confidence to an independent person. A whistle-blowing system is therefore a form of internal control that seeks to reduce the risk that information about wrongdoing by employees will not go unreported and undetected

A.2.9. Information processing controls

An essential objective for any business organization should be to ensure the integrity of its information systems, and that the information produced by the organization is accurate and reliable. Information systems provide information to management, so that they are aware of what is happening in the organization and can make decisions. The information provided by a company to its shareholders and to the government and regulatory authorities must also be reliable and trustworthy

Inadequate information or incorrect information inevitably creates problems for management and for the efficiency of business operations. It is therefore extremely important that information should be processed and recorded accurately. Information processing controls are a key feature of an internal control system

Controls over the processing and storage of information are needed because there are risks not only of errors, but also of unauthorized access. The risks of errors are much greater in some information systems than in others

Manual and automated controls

Manual controls are controls that are applied by human activity or intervention. Automated controls are controls that are activated without any human intervention. Automated controls are more robust and reliable than manual controls, because humans can easily make mistakes or omissions. However, where manual controls are used rather than automated controls, it is important to try to make the controls as effective as possible

A.2.10. Monitoring an internal control system

The effectiveness of the IC system should be reviewed. Reviews should be made regularly by management and at least annually by the board of directors or the audit committee of the board

Internal control systems should be monitored regularly, to check whether the system remains effective and whether controls remain sufficient to achieve their control objective.

The outcome of reviews of the internal control system in companies should be reported to the board of directors

The outcome of a review of the system may be any of the following

Identified by monitoring process	Subsequent action
Controls that have not been properly implemented	The individuals responsible for the controls will be informed of their failure
Controls that are not fulfilling their intended purpose because of design weaknesses in the control	The managers responsible for the control should design more effective controls
New risks have emerged and there are insufficient controls for dealing with them	The managers responsible for the control should design more effective controls. The managers responsible for risk assessment should review the adequacy of the processes for risk identification, analysis and evaluation
Some existing controls are no longer required because circumstances have changed	The managers responsible for the control should be advised
Information about controls is not reported to the relevant individuals as promptly as it should be	Responsible management should be informed accordingly

In a company, the board of directors has the final responsibility for the effectiveness of the internal control system. However, managers are given the responsibility for designing and implementing the control system, so they too have responsibilities for ensuring that controls are effective

How does the board of directors monitor the effectiveness of the internal control system	How does senior management monitor the effectiveness of the internal control system
The board may delegate responsibility for monitoring to an audit committee	Senior management may establish management risk committees to review risks and control within the business operations
The board or audit committee should obtain information about the effectiveness of controls from: <ul style="list-style-type: none"> ✓ Senior management reports ✓ External auditors (who should report on financial internal control weaknesses after they have completed the annual audit) 	Senior management or the risk management committee should obtain information about the effectiveness of controls from: <ul style="list-style-type: none"> ✓ Direct observation and experience ✓ Reports from other risk management committees in the company ✓ External auditors

<p>✓ Internal auditors. If the company has an internal audit department, the internal auditors check the effectiveness of internal controls, at the request of the board/audit committee and also management</p>	<p>✓ Internal auditors, if the company has an internal audit function</p>
--	---

A.2.11. Limitations of an internal control system

An IC system has inherent weaknesses. It can provide only reasonable assurance that the controls are effective in achieving their objectives, not absolute assurance

Internal control systems have several inherent limitations.

- The effectiveness of an internal control depends on the strength of the risk awareness culture in the organization. If directors and senior management fail to provide effective leadership on risk control, the internal control system will not be as effective as it should be.
- Internal controls may reduce operational risks, but they cannot prevent operational failures and errors.
- Controls may not be properly implemented, so that the controls are not applied in the intended way
- Operational risks change because there are continual changes and developments in the business environment. These changes create new internal risks (as well as new external risks). Existing internal controls may not be sufficient to deal with the new risks.
- Internal controls cost money to design and implement. Sometimes the additional benefits from an internal control do not justify the cost of the control.
- Two or more employees may collude to override a control. In particular, segregation of duties can be overridden if the performers of each duty collude.
- Management may use their authority to override the controls.
- Unusual transactions may not be effectively captured by controls which are usually designed based on routine transactions.
- Human error may prevent a control from working, particularly where judgement is involved.
- Controls may fail or breakdown. For example, computer-based controls may not operate effectively if one or more software packages fails

A.2.12. Governance and risk

The board of directors has final responsibility for the effectiveness of the IC system, and in listed companies, the board is accountable to shareholders for this

Governance is a term for the leadership provided to an organization. Corporate governance is governance in companies

The board of directors govern the company on behalf of its owners, the shareholders. They are accountable to the shareholders for the performance of the company and its success in achieving its objectives. Accountability is provided through the requirement to prepare the annual report and accounts and the annual general meeting of the company

To fulfil their responsibilities to the shareholders, the board of directors should provide effective leadership to the company. The board decides the objectives of the company, which often include objectives for financial growth or profitability; but the board should also ensure that in the pursuit of its objectives, the company does not expose itself to excessive risks

Governance: board responsibilities for internal control Responsibilities for internal control within a company may be stated as follows.

- The board of directors is responsible for ensuring that the company has an effective internal control system.
- The Code of Best Practice on Corporate Governance (2017) sets out clearly the governance responsibilities of the board of directors of these companies for internal control. This sets out clearly the governance responsibilities of the board of directors of these companies for internal control.
- The board of directors should have a sound system of internal control to safeguard the investments of their shareholders and to safeguard the company's assets.
- The internal control system should provide reasonable assurance (but not absolute assurance) regarding the achievement of the company's objectives.
- The board should review the design and effectiveness of the system of internal control.
- The annual report of the company should include a sub report by the board about the effectiveness of the internal control system. This report should include acknowledgement by the board of its responsibility for the system. It should also disclose the process for dealing with any significant problems with internal control that have been discovered.
- There should be an ongoing system for identifying, evaluating and managing significant risks. An important point to note is that the effectiveness of internal control in a company is the responsibility of the board of directors

Responsibilities of management for internal control

Management are given the delegated responsibility for designing and implementing the control system, and they are accountable to the board

The board delegates operational responsibility for internal control to management, and management should be accountable to the board for the effectiveness of internal control

Management is responsible for introducing controls into an organization.

- They should approve the design of controls.
- They should ensure that controls are implemented properly.
- They should ensure that control information is communicated to relevant persons.
- They should review the effectiveness of controls and report to the audit committee or the board. The responsibility of management for internal control is to the board, however, and not to the company's shareholders

Responsibilities of auditors for internal control

External and internal auditors provide management with information and recommendations about internal controls

The Code of Best Practice in Corporate Governance (2017) states that companies should have an internal audit function. Internal auditors investigate control systems and report to management, the audit committee or the board about their findings and recommendations. However, internal auditors do not have ultimate responsibility for internal control

External auditors consider the effectiveness of internal financial controls, as part of the annual audit process. They should report to management and the audit committee about any weaknesses in internal financial controls that they discover. However, the external auditors do not have direct responsibility for internal control but they should report deficiencies in internal control as required by auditing standards



Chapter review questions

1. Internal controls are designed to reduce _____.
2. What are the five elements of the COSO internal control system framework?
3. In a bank, foreign exchange transactions are made by FX traders, but transactions are settled by someone in the bank's back office.
This is an example of what type of control procedure?
4. Which two of the following types of internal control relate to a prominent notice on a building construction sign warning all people on the site to wear a hard hat, as required by health and safety regulations?
 - A Operational control
 - B Compliance control
 - C Preventive control
 - D Detective control
5. One way of applying internal control through segregation of duties is to separate responsibilities for four different functions: (1) _____ (2) _____ (3) _____ and (4) _____
6. An internal control may fail to achieve the objective for which it was intended. This is known as an _____ risk

