TOPIC 2

INTERNAL CONTROL

Topic overview

In the previous topic you learnt about **corporate governance and statutory matters**. The aim of this topic is to explain and apply the theory of internal control as an important aspect of corporate governance. It will be explained according to the objectives of internal control and the components of internal control in chapter 5 of Jackson & Stent. General and application controls in a computerised environment will also be explained and applied as part of control activities in chapter 8 of Jackson & Stent.

The need for the external auditor to obtain an understanding of a client's internal control in order to identify significant risks will also be explained.

This topic is divided into the following learning units:

	Learning unit	Title
	2.1	**Internal control**
	2.1.1	Definition of internal control
	2.1.2	Limitations of internal control
	2.2	**Components of internal control**
	2.2.1	Control environment
	2.2.2	Risk assessment
	2.2.3	Information system
	2.2.4	Control activities
	2.2.5	Monitoring of controls
	2.3	**Controls in a computerised environment**
	2.3.1	General controls
	2.3.2	Application controls
	2.4	**Internal control from the perspective of the external auditor**
	2.4.1	Obtaining an understanding of internal control
	2.4.2	Significant risks

Learning outcomes

Learning unit	In this topic we focus on the following learning outcomes:	Level
2.1 Definition of Internal control	• Define and explain internal control	2
	• Explain the limitations of internal control.	2
2.2 Components of internal control	• Describe, explain and apply the five components of internal control.	2
2.3 Controls in a computerised environment	• Describe, explain and apply general controls in a computerised environment	2
	• Explain and apply application controls in a computerised environment.	2
2.4 Internal control from the perspective of the external auditor	• Explain the need for the external auditor to obtain an understanding of a client's internal control in order to identify significant risks.	2

LEARNING UNIT 2.1

INTERNAL CONTROL

INTRODUCTION

The importance of good corporate governance to a business and its stakeholders was explained in topic 1. As part of Principle 3.8, point 65.1, of the King III Report (2009:64) it is stated that **the audit committee should be responsible for overseeing financial risk management and controls and ensuring that the controls provide guidance that embeds internal financial control in the business processes and evolves to remain relevant over time.**

2.1.1 DEFINITION OF INTERNAL CONTROL

As stated in Jackson & Stent (2014:5/3) internal control is designed to address and limit potential risks.

STUDY

Jackson & Stent (2014:5/3–5/4) Section 1

ACTIVITY 1

Name and explain six key characteristics of internal control that you have learnt.

FEEDBACK ON ACTIVITY 1

Reference: Jackson & Stent (2014:5/4) Section 1.3

The characteristics of internal control are:

- Internal control is a process.
- Internal control is effected by people.
- Internal control is not the sole responsibility of management.
- Internal control is not static.
- Internal control is not fool proof.
- Internal control is not a case of a single control addressing a single risk.

From the above aspects of internal control it is clear that although the board of directors is responsible overall for the governance of risk, everyone in the business carries responsibility with regards to the implementation and execution of internal controls.

The board of directors has the overall responsibility and accountability. Management identify risks, design and implement policies and procedures to address risks, while the employees execute internal control procedures. Therefore, it is clear to see that success depends on all parties involved.

STUDY

Jackson & Stent (2014:5/5) Section 3

ISA 315.4(c) **defines internal control** 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

* the reliability of the entity's financial reporting
* the effectiveness and efficiency of its operations, and
* its compliance with applicable laws and regulations

2.1.2 LIMITATIONS OF INTERNAL CONTROL

Your prescribed textbook, Jackson & Stent (2014:5/4), correctly indicates that internal control does not provide absolute assurance that the risks, that threaten the achievement of the objectives of the business, will be adequately responded to. This is due to the inherent limitations of internal controls.

STUDY

Jackson & Stent (2014:5/4–5/5) Section 2

ACTIVITY 2

Management design an internal control system, which **theoretically** addresses risk. List six limitations of inherent control and provide an example of each.

FEEDBACK ON ACTIVITY 2

Reference: Jackson & Stent (2014:5/4 - 5/5)

The inherent limitations of internal control and examples thereof are explained in your textbook under section 2 and are not repeated here.

SUMMARY

In this learning unit we explained the definition and limitations of internal control. We also explained that internal control is a response to risk and that the entity's objectives are achieved by implementing **internal controls**.

LEARNING UNIT 2.2

COMPONENTS OF INTERNAL CONTROL

INTRODUCTION

Internal control consists of the following five components (Jackson & Stent 2014:5/5–5/6):

1. Control environment
2. Risk assessment
3. Information systems
4. Control activities
5. Monitoring of controls

Internal controls in a computerised environment are part of the system of internal control of an entity. It is important to keep this in mind when studying the components of internal control below. **General and application controls** in a computerised environment will be explained in detail in learning unit 2.3.

STUDY

Jackson & Stent (2014:5/5–5/6) Section 4
Jackson & Stent (2014:8/4–8/6) Section 2

The five components of internal control will now be explained in more detail.

2.2.1 CONTROL ENVIRONMENT

STUDY

Jackson & Stent (2014:5/7–5/8) Section 4.1

As stated in Jackson & Stent (2014:5/7) the control environment sets the tone of the entity and creates the atmosphere in which employees go about their duties. The desirable mind set is one of "**doing things the right way**".

2.2.2 RISK ASSESSMENT

The King III Report (2009:76) states that the board should ensure that risk assessments are performed on a continual basis. It also states under principle 5.5 that information technology risks form an integral part of the company's risk management activities.

STUDY

Jackson & Stent (2014:5/8–5/10) Section 4.2

Risk assessment is important because internal controls are designed and implemented as a response to assessed risks. It is therefore critical that the risk assessment process is comprehensive, accurate, thorough and complete.

2.2.3 INFORMATION SYSTEM

Your prescribed text book Jackson & Stent (2014:5/10) explains the objective of the information system and its subpart, the accounting system, to produce information that is **valid** (the transactions and events underlying the information actually **occurred** and were **authorised**), **accurate** and **complete** and timeously produced.

STUDY

Jackson & Stent (2014:5/10–5/12) Section 4.3

2.2.4 CONTROL ACTIVITIES

The entity's objective relating to financial reporting to record and process only transactions (and events) which have occurred and pertains to the entity and which are recorded and processed accurately and completely can only be realised in the information system with the implementation of control activities. This will now be explained.

2.2.4.1 General principles

Control activities are the **actions** which are carried out to manage or reduce risks (Jackson & Stent 2014:5/12) and to achieve the entity's objectives of providing reliable financial reporting, have effective and efficient operations and to comply with the laws and regulations.

STUDY

Jackson & Stent (2014:5/12–5/17) Section 4.4

Note the following types of control activities:

- Approval, authorisation
- Segregation (division) of duties
- Isolation of responsibility
- Access/custody (security)
- Comparison and reconciliation
- Performance reviews

Also note that the control activities can be **preventive**, **detective** or **corrective** in nature.

ACTIVITY 1

Twinkles Groceries (Pty) Ltd

Twinkles Groceries (Pty) Ltd (hereafter referred to as Twinkles) is a large local grocery store. At the start of a cashier's shift, the cashier must use a username and password to log onto his/her till. If the cashier accidentally makes a mistake, for example, scan an item twice, he/she has to call the manager to authorise a correction. The manager will first ask what happened and determine if the information provided is true, before entering a password. When all the items have been scanned, the total amount due is automatically calculated and shown on the screen. At the door to the store, a security guard will check the customer's bag of groceries against the customer's till slip.

Identify the internal controls implemented by Twinkles and link each of them to a type of control activity.

FEEDBACK ACTIVITY 1

No	Internal control	Type of control activity
1.	The cashier uses a username and password to gain access to the till.	**Isolation of responsibilities** (remember, there are normally more than one cashier), **access controls**
2.	A manager has to authorise any corrections of mistakes made.	**Segregation of duties** between the manager functions and the cashier duties, approval and authorisation
3.	The security guard checks the goods in the bag to the till slip.	**Comparison and reconciliation**

ACTIVITY 2

1. For each of the six types of control activities, give an example of **what could go wrong (risks)** in the absence of the control activity.

2. Clearly indicate the difference between **segregation of duties** and **isolation of responsibilities**.

FEEDBACK ON ACTIVITY 2

Reference: Jackson & Stent (2014:5/12–5/16)

1. The following table provides a list of **possible things that could go wrong (risks)** in an accounting system for each of the types of control activities. This is based on the examples given in Jackson & Stent (2014:5/12–5/16).

Control activity	Things that could go wrong (risks)
Approval, authorisation	Credit sales could be made to customers who are not credit worthy and who cannot pay their accounts, if a credit sale is not approved by the credit controller first.
Segregation of duties	Goods purchased could be stolen if no segregation of duties exists between the authorisation of the order, the placing of an order and the issuing the goods received note, as the purchase clerk could order it for him/herself whilst letting the company pay.
Isolation of responsibility	An incorrect number of goods could be received if a supplier delivers goods to a company and the receiving clerk does not count the goods and sign the supplier's delivery note. The clerk could not be held responsible and the mistake could be repeated.
Access/ custody	Physical inventory could be stolen if not stored properly, for example if not protected by a security guard at the inventory warehouse entrance.
Comparison and reconciliation	The balance of the cash receipts and payments journal could be incorrect if it is not regularly compared and reconciled to the balance on the bank statement.
Performance reviews	An abnormal increase in transport costs due to fuel being stolen could go undetected due to management not comparing the actual cost figure to the budgeted transport cost.

Note that these risks are examples based on your study material and that there are many other possible solutions.

2. **Segregation of duties** is an internal control designed to reduce error and fraud by ensuring that at least two individuals are responsible for the separate parts of a task. For example, the sales order clerk will receive

an order, but the sales manager has to authorise the sale before the clerk can process/record the order.

Isolation of responsibilities refers to the accountability of an employee for a specific task, and the acknowledgement by the employee for the performance of an internal control. This is normally done by signing. In other words, there could be more than one sales order clerk who takes orders. The signature can isolate who was responsible for a task (should a problem arise) and the employee acknowledges the performance of an internal control procedure. It could also signify the transfer of responsibility from one individual to the next in the task process.

2.2.5 MONITORING OF CONTROLS

As stated in Jackson & Stent (2014:5/17) the monitoring of controls involves the assessment of internal control performance over time. If controls are not monitored, the board or management will not know if the entity's financial reporting is reliable and whether the laws, regulations and company policies are being complied with.

STUDY

Jackson & Stent (2014:5/17–5/18) Section 4.5

ACTIVITY 3

Internal control

You have been assigned to the task of completing the firm's internal control questionnaire. The following policies and procedures implemented have been noted regarding the internal control of SoftWorld (Pty) Ltd.

a) Regular meetings are held at divisional and departmental levels to consider the risks at specific levels within the organisation.

b) Weekly reports on invoicing and debt collection are produced by the online system and are reviewed by management.

c) When goods are delivered by a supplier, the receiving clerk counts the goods and then signs the delivery note as proof that he was responsible for receiving the delivery.

d) From inspection of the minutes of the board of directors' meetings it appears as though all directors are involved in the decision-making process.

e) Procedures are in place to resolve incorrect processing of transactions.

f) The entity operates within specific operating guidelines and time is taken by management to create and implement systems and procedures.

Based on the information given regarding the entity's internal control:

1. **List** the **five (5)** components of internal control.
2. For each of the policies and /or procedures described in (a) to (f) in the scenario, **identify** the relevant component of internal control it relates to.

FEEDBACK ON ACTIVITY 3

1 Components of internal control

Control environment

The entity's risk assessment process

The information system

Control activities

Monitoring of controls

2

Policies and /or procedures(a)-(f)	Component of internal control
a)	The entity's risk assessment process/control environment
b)	Monitoring of controls/control activities/control environment/ the information system
c)	Control activities
d)	Control environment
e)	The entity's information system and related business processes/control environment
f)	Control environment

SUMMARY

In this learning unit we explained the five components of internal control.

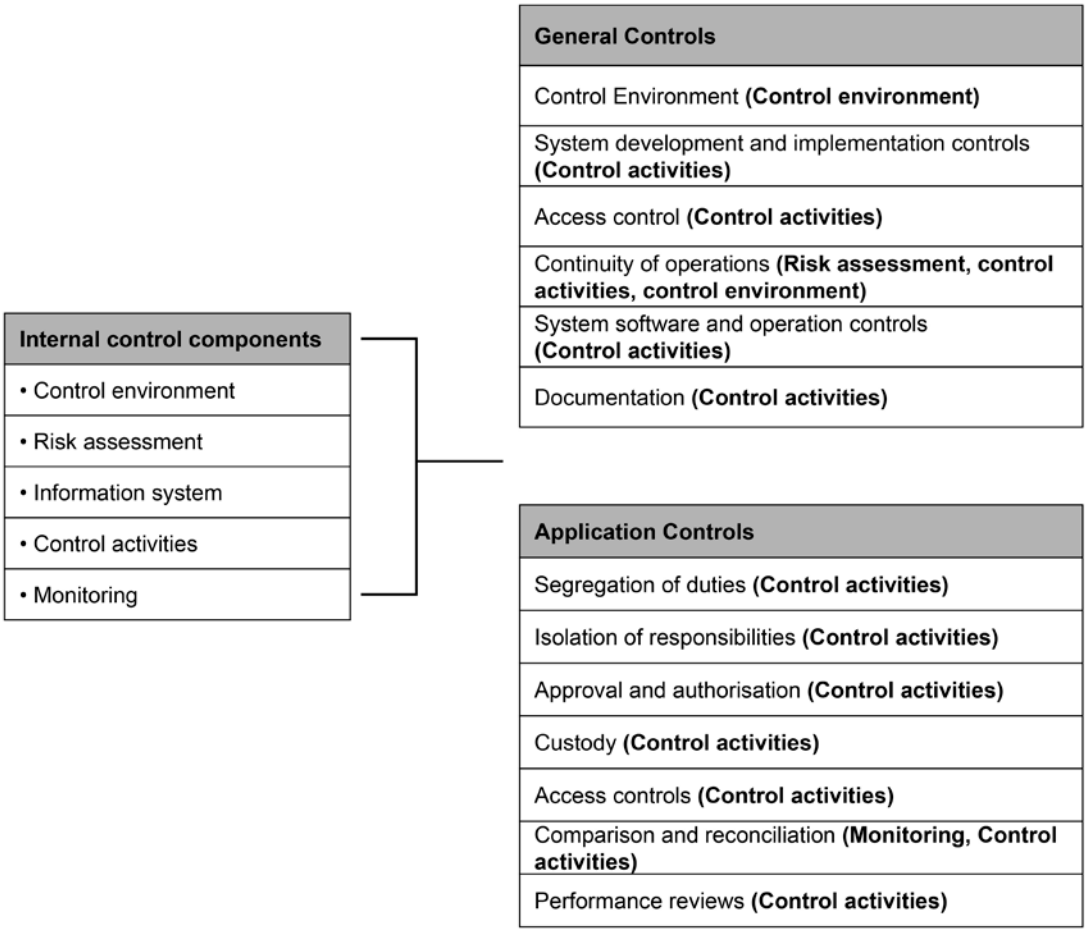
LEARNING UNIT 2.3

CONTROLS IN A COMPUTERISED ENVIRONMENT

INTRODUCTION

General and application controls in a computerised environment are an integral part of the total system of internal control of an entity and touch on all components of internal control.

The following diagrammatic representation of general and application controls illustrates that the general and application controls relate to all the components of internal control.



Diagrammatic representation of general and application controls

Although the information system component is not evident under general and application controls, the information system underlies internal controls in a computerised environment, as this is where the controls are implemented.

General and application controls can be **manual** or **computerised**.

STUDY

Jackson & Stent (2014:8/3–8/4)

General and application controls are discussed in more detail in the sections to follow.

2.3.1 GENERAL CONTROLS

General controls are defined as those controls which establish an **overall framework** of control for computer activities, and they span across all applications (Jackson & Stent 2014:8/7, section 1). General controls are of great importance. As general controls operate "around" the application controls, if your general controls are not adequate, the application controls might not be of much use.

Note the following:

- The term "computerised environment" refers to any particular and unique combination of hardware, software and personnel (Jackson & Stent 2014:8/3).

STUDY

Jackson & Stent (2014:8/7–8/25)

ACTIVITY 1

Access controls in a computerised environment are important as the consequences of unauthorised access to a system can be disastrous for a company.

REQUIRED

1. Describe the **general physical access controls** that should be present to ensure proper internal control in a computerised environment.
2. Give examples of **preventative logical access controls** in a computerised environment.
3. Explain what controls over passwords as part of **logical access controls** entails.

FEEDBACK ON ACTIVITY 1

Jackson & Stent (2014: 8/17–8/20)

1. Interpret the question as follows:
   - It requires **general controls** (not application controls).
   - It requires **access controls**.
   - It requires only **physical** access controls (not logical access controls).

   General physical access controls includes aspects such as:

   - control over visitors from outside the company to the IT building, for example they should be escorted to the IT department
   - controlled access to company personnel other than IT personnel
   - physical entry to the data centre to be controlled, for example closed circuit televisions (CCTVs) at entrances
   - access control over remote workstations/terminals, for example terminals should be secured to desks

2. Apply the steps in 1. to interpret the question.

   All **logical access** controls are preventative in nature and consist of the following:

   - identification of users and computer resources
   - authentication of users and computer resources
   - authorisation of the levels of access to be granted
   - logging of access and access violations
   - access tables

3. Control over passwords is fundamental to successful, logical access controls. This is explained in your textbook under section 5.4 and is not repeated here.

2.3.2 APPLICATION CONTROLS

Jackson & Stent (2014:8/26) defines application controls as any control **within** an application which contributes to the accurate and complete recording and processing of transactions which have actually occurred, and have been authorised (**occurred**, **accurate** and **complete** information).

The stages through which a transaction flows through the system can be described as **input, processing** and **output** and application controls can be described in terms of these activities, e.g. an application control relating to **input**.

In addition to implementing controls over input, processing and output, controls must be implemented over **masterfiles**. A masterfile is a file which is used to store only standing information and balances, e.g. the debtors

masterfile will contain the debtor's name, address, contact details, credit limit etc. The masterfile is a very important part of producing reliable information and must be strictly controlled.

The objective of controls in a computerised accounting environment is generally regarded as being centred around the occurrence, authorisation, accuracy and completeness of data and information processed by and stored on the computer.

Occurrence and authorisation are concerned with ensuring that transactions and data

- are not fictitious (they have occurred) or fraudulent in nature, and
- are in accordance with the activities of the business and have been properly authorised by management

Accuracy is concerned with minimising errors by ensuring data and transactions are correctly captured, processed and allocated.

Completeness is concerned with ensuring that data and transactions are not omitted or incomplete.

STUDY

Jackson & Stent (2014:8/26–8/41) Sections 1–4

ACTIVITY 2

The following control techniques and application controls, applicable to the **input stage** through which a transaction flows through the system, are mentioned in your textbook, Jackson & Stent (2014: 8/27–8/40):

Access control
Authorisation
Batching
Screen aids and related features
Programme controls relating to input
Existence/validity checks

- Validation checks
- Matching checks
- Data approval / authorisation checks
- Reasonableness and limit checks
- Dependency checks
- Format checks
- Check digits
- Sequence checks

Logs and reports

- Override reports
- Activity reports
- Access/access violation reports

- Audit trails

REQUIRED

Link the control techniques and application controls mentioned to the **objective of the control** being either occurrence and authorisation, completeness or accuracy.

FEEDBACK ON ACTIVITY 2

Jackson & Stent (2014:8/27–8/40) Sections 1–4

Input controls

Occurrence and authorisation	Completeness	Accuracy
1. Access control 2. Authorisation 3. Batching 4. Existence / validity checks for example • Validation checks • Matching checks • Data approval / authorisation checks 5. Logs and reports for example • Override reports • Activity reports • Access / access violation reports	1. Batching 2. Sequence tests 3. Logs and reports, for example: • audit trails	1. Batching 2. Screen aids and related features, for example: • Minimum keying in of information • The screen should be formatted • Screen dialogue and prompts • Mandatory fields • Shading of fields 3. Reasonableness and limit tests 4. Dependency checks 5. Format checks, for example: • Alpha-numeric • Size checks • mandatory field/missing data checks • Valid character and sign check 6. Check digits

Please remember that the suggested solution is only a **checklist** for study purposes. In tests and exams you should expand on the above, for example

"The computer should perform a sequence test on invoice numbers and print an exception report if there are any outstanding invoices". This will be illustrated when applied to the various business cycles in the topics to follow.

Follow these steps:

1. Determine at which stage in the scenario a transaction flows through the system. Which of the following does the scenario deal with?

    - input phase
    - processing phase, and/or
    - output phase

2. Determine the objective of the control to be addressed. Which of the following does the question require you to address?

    - occurrence and authorisation
    - accuracy, and/or
    - completeness

ACTIVITY 3

Describe the application controls that the management of company X should implement to ensure the completeness of amendments to a masterfile in the computerised accounting system.

FEEDBACK ON ACTIVITY 3

Objective of the controls	**Masterfile amendments**
Completeness	1. All amendments should be recorded on hardcopy masterfile amendment forms (MAF) (no verbal instructions). 2. MAFs should be pre-printed, sequenced and designed in terms of sound document design principles. 3. All masterfile amendments should be automatically logged by the computer on **sequenced** logs. 4. The MAFs themselves should be **sequence checked** against the log to confirm that all MAFs were entered.

SUMMARY

In this learning unit we explained general and application controls in a computerised environment as part of a system of internal control.

LEARNING UNIT 2.4

INTERNAL CONTROL FROM THE PERSPECTIVE OF THE EXTERNAL AUDITOR

INTRODUCTION

The external auditor obtains an understanding of a client's system of internal control as part of his/her external audit.

2.4.1 OBTAINING AN UNDERSTANDING OF INTERNAL CONTROL

Jackson & Stent (2014:7/14) states that an understanding of a client's internal control assists the auditor in identifying types of potential misstatement and factors that affect the **risks of material misstatement**, and in designing the nature, timing and extent of further audit procedures.

STUDY

Jackson & Stent (2014:7/14–7/19)

2.4.2 SIGNIFICANT RISKS

Jackson & Stent (2014:7/19) defines significant risks as risks that require special audit consideration. Such risks relate to the auditor's risk of material misstatement. The auditor assesses risk so that he or she can determine the nature, timing and extent of further audit procedures.

STUDY

Jackson & Stent (2014:7/19–7/20) Sections 1-3

ACTIVITY 1

Name the six factors that the auditor should consider when assessing whether a risk is a significant risk.

FEEDBACK ON ACTIVITY 1

Reference: Jackson & Stent (2014:7/19)

The six factors that the auditor should consider when assessing whether a risk is a significant risk are explained in your textbook and are not repeated here.

SUMMARY

In this learning unit we explained the need for the external auditor to understand internal control in order to identify significant risks.

CONCLUSION

In this topic, **Internal control**, we explained and applied the theory of internal control according to the five components of internal control. We explained that internal control is designed to address and limit potential risks. Internal control from the perspective of the external auditor was also explained.