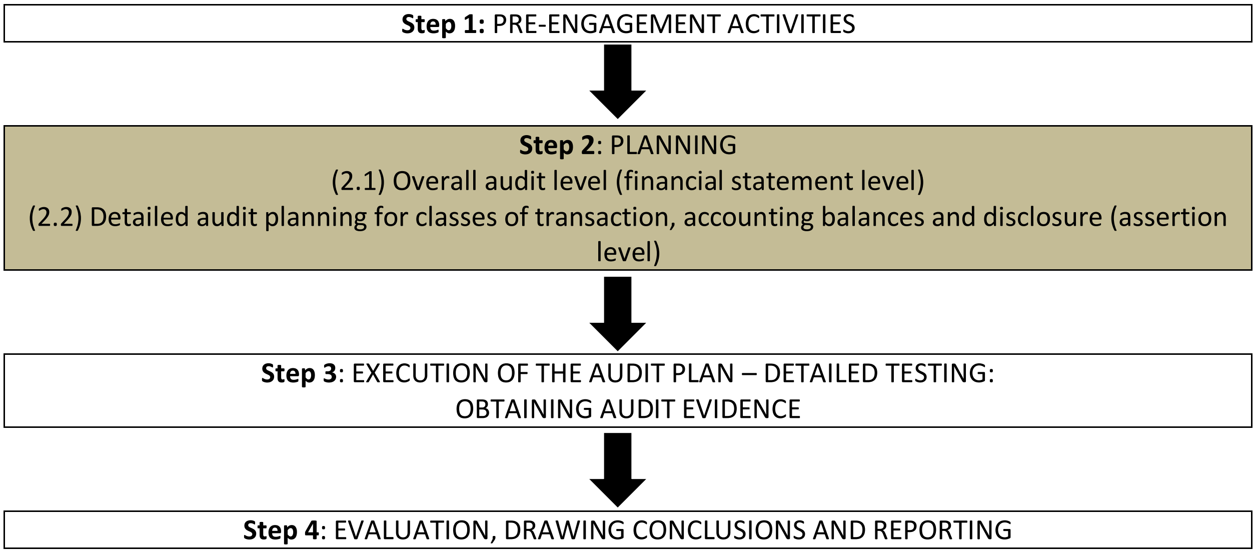
ASPECTS OF INTERNAL CONTROL OF IMPORTANCE TO AN AUDITOR

(AUE301P)

Study Unit 2.1

Background to internal control

A schematic representation of the audit process:



Step 1: PRE-ENGAGEMENT ACTIVITIES

Step 2: PLANNING
(2.1) Overall audit level (financial statement level)
(2.2) Detailed audit planning for classes of transaction, accounting balances and disclosure (assertion level)

Step 3: EXECUTION OF THE AUDIT PLAN – DETAILED TESTING:
OBTAINING AUDIT EVIDENCE

Step 4: EVALUATION, DRAWING CONCLUSIONS AND REPORTING

During the planning phase of the audit, the auditor identifies the risk of material misstatement at the financial statement level and the individual statement level (for material class of transactions, balances and disclosure).

Internal control has the following influence on the audit:

1. **While performing the risk assessment procedures the auditor does the following**:
    - Obtains an understanding of the internal control at the enterprise
    - Evaluates the design of the entity's internal controls & determines whether it has been implemented. The auditor should determine whether a control would be sufficient to effectively prevent, detect & correct material misstatement. This would also help the auditor to decide on the nature, timing and extent of any further audit procedures that are required.
2. **While performing further procedures in response to the assessed risks the auditor would do the following**:
    - Perform tests of control since the auditor is of the opinion that the execution of substantive procedures alone is not sufficient to provide relevant audit evidence, because it would not be possible or practical to reduce the risk of material misstatement at the statement level by carrying out substantive procedures alone.
    - Perform tests of control when he expected the risk of material misstatement to be low because the company had effective controls in place.

Step 1: Preliminary stage (Pre-engagement activities)

These are activities which take place before an audit engagement is accepted. They include:

- Determining whether the audit firm wishes to establish or continue the client relationship;
- Establishing whether the client can be appropriately serviced;
- Evaluating whether the firm is able to comply with the ethical requirements relating to the engagement, e.g. is there a threat to independence?;
- Establishing an understanding of the terms of the engagement.

Step 2: Planning stage

The activities within this stage include:

- Establishing the audit strategy – the scope, timing and direction (focus) of the audit will be and what resources will be needed on the audit;
- Considering materiality – auditor making judgment about the size of misstatements which will be material;
- Planning risk assessment procedures – this entails planning the procedures which will be conducted to obtain an understanding of the entity and its environment;
- Conducting risk assessment procedures – this entails carrying out the planned risk assessment procedures & identifying & assessing the risk of material misstatement as they progress;
- Planning "further" and "other" audit procedures – planning procedures which will be conducted to address the identified risks, in such a manner that audit risk (**the risk of giving an inappropriate opinion**) is reduced to an acceptable level.

The auditor in effect develops one audit plan with two sections, namely:

- ***Section 1*** will describe the nature, timing and extent of procedures to **identify and assess risk**;
- ***Section 2*** will describe the nature, timing and extent of **further audit procedures** which are needed to respond to the risks identified; and
- ***Section 2*** will also describe **other audit procedures** which must be carried out to ensure that the audit complies with the ISAs.

Step 3: Responding to assessed risk stage

ISA 330 states that the auditor should obtain sufficient, appropriate audit evidence regarding the assessed risks of material misstatement through designing and implementing appropriate responses to those risks. The auditor's first response to assessed risk is to ***plan*** "further" and "other" audit procedures & thereafter –

- Respond to assessed risk at **financial statement level**, e.g. assigning appropriately experienced and skilled individuals to the audit team to execute the plan;
- Respond specifically to assessed risk at ***assertion level*** by carrying out tests of controls and substantive tests in order to gather sufficient, appropriate evidence that material misstatement has not gone undetected; and
- ***Carry out*** those procedures which are required to comply with the ISAs.

Step 4: Concluding stage

This stage of the process consists of:

- Evaluating and concluding on the audit evidence gathered – this means evaluating all the audit evidence gathered to determine whether it is sufficient and appropriate to draw a conclusion of fair presentation;
- Formulating the audit opinion & drafting the audit report which conveys that opinion.

The influence of internal control on the audit process

REASONS WHY THE OBTAINING OF AN UNDERSTANDING OF THE ACCOUNTING AND INTERNAL CONTROL SYSTEMS FORMS PART OF THE AUDIT PROCESS

The objective of an audit of financial statements is to enable the auditor to express an opinion as to whether or not the financial statements fairly present, in all material aspects, the financial position of the entity at a specific date, and the results of its operations & cash flow information for the period ended on that date, in accordance with an identified financial reporting framework.

When an auditor studies the accounting & internal control systems, he gains knowledge of the design & operation of the systems.

The knowledge and understanding of the accounting & internal control systems that are applicable to all the transactions and balances will therefore assist the auditor to:

- Evaluate the adequacy & suitability of the systems;
- Formulate the most suitable audit approach based on the accounting & internal control systems, in other words, decide on the nature, timing & extent of the tests of internal controls & the substantive procedures;
- Plan the audit efficiently;
- Understand control risk & design audit procedures accordingly;
- Express an opinion on the financial statements

FINANCIAL STATEMENT ASSERTIONS

Financial statement assertions are assertions which management makes on the financial statements submitted to the auditor. Examples would be assertions made by management that the information in their statements is complete, accurate, correctly classified & correctly valued.

In order to express an audit opinion on the fair presentation of the financial statements, the auditor collects audit evidence to substantiate each statement for classes of transactions, account balances and presentation & disclosure.

This procedure involves the **audit objectives**. Audit objectives are the criteria against which the auditor measures the information in the financial statements to determine whether management's assertions relating to the financial statements are valid. These audit objectives therefore revolve around the assertions in the financial information & are derived directly from management's assertions in the financial statements. The audit objectives represent what the auditor wants to achieve by performing an audit of the financial statements.
Financial statement assertions can be divided into the following categories:

- assertions concerning the classes of transactions and events
- assertions concerning account balances
- assertions concerning presentation and disclosure

The following is a summary of the specific assertions that management makes with regard to transactions, events, balances and presentation & disclosure:

Assertion	**Transactions & events**	**Balances: assets, liabilities & equity interests**	**Presentation & disclosure**
Occurrence	X		X
Completeness	X	X	X
Accuracy	X		X
Cut-off	X		
Classification	X		X
Existence		X	
Rights & obligations		X	X
Valuation & allocation		X	X

1.1 Assertions about classes of **transactions and events** for the period under audit:

▪

a) **Occurrence**: transactions & events that have been recorded, have occurred & pertain to the ▪ entity.

b) **Completeness**: all transactions & events that should have been recorded, have been recorded.

c) **Accuracy**: amounts relating to recorded transactions & events, have been recorded ▪ appropriately.

d) **Cut-off**: transactions & events have been recorded in the correct accounting period.

e) **Classification**: transactions & events have been recorded in the proper accounts.

1.2 Assertions about **account balances** at the period end:

a) **Existence**: assets, liabilities & equity interests exist.

b) **Rights & obligations**: the entity holds or controls the rights to assets, and liabilities are the obligations of the entity.

c) **Completeness**: all assets, liabilities & equity interests that should have been recorded, have been recorded.

d) **Valuation & allocation**: assets, liabilities and equity interests are included in the financial statements at appropriate amounts & any resulting valuation or allocation adjustments are appropriately recorded.

1.3 Assertions about **presentation and disclosure**:

a) **Occurrence and rights and obligations**: disclosed events, transactions, and other matters have occurred & pertain to the entity.

b) **Completeness**: all disclosures that should have been included in the financial statements, have been included.

c) **Classification & understandability**: financial information is appropriately presented & described, and disclosures are clearly expressed.

d) **Accuracy & valuation**: financial & other information are disclosed fairly & at appropriate amounts.

Example 1:

When the auditor gathers evidence about **sales transactions,** he will be seeking evidence to support the following assertions:

- **Occurrence**: all sales included are genuine sales (not fictitious) of the entity (a genuine sale of the company's goods / services have occurred);
- **Completeness**: all sales which were made, have been included in the total of sales made for the year;
- **Accuracy**: all sales have been recorded appropriately, this implies prices are correct & that the correct discount & VAT rates have been used & correctly calculated;
- **Cut-off**: all sales recorded, occurred in the accounting period being audited;
- **Classification**: all sales have been posted to the proper account. This implies that a credit sale has been posted to the correct debtor's account & that VAT has also been correctly posted.

The assertions which DO NOT apply to sales are **existence, valuation** and **rights & obligations**. Why is this? These 3 assertions apply to **balances** in the balance sheet which are carried forward to the following period, and not to **transactions**.

Example 2:

When the auditor gathers evidence about **plant & equipment**, he will be seeking evidence to support the following assertions:

- **Completeness**: all plant & equipment owned by the company, is included in the balance reflected in the financial statements;
- **Existence**: all plant & equipment included in the balance, existed at balance sheet date;
- **Valuation & allocation**: the plant & equipment has been reflected in the balance sheet at appropriate amounts; this means that reasonable adjustments have been made for depreciation, impairment and obsolescence;
- **Rights**: the company has right of ownership to the plant & equipment reflected in the balance sheet.

The assertions which do not apply to plant & equipment are **occurrence** and **accuracy, cut-off** and **classification**. Why is this? It is because these assertions apply only to transactions/events and not to balances contained in the balance sheet.

Once the auditor has gathered sufficient, appropriate evidence relating to the financial statement assertions, he will be in a position to evaluate the evidence & express an opinion on the fair presentation of the financial statements.

2. INTERNAL CONTROL FROM A BUSINESS PERSPECTIVE

Objectives for a business are set & the risks relating to achieving those objectives will be identified and suitable measures will be put in place to address those risks. This will include addressing the risks associated with matters like:

- Safeguarding the assets of the company, e.g. inventory, from theft or damage
- Preventing fraud
- Complying with the laws & regulations applicable to the entity
- Producing reliable financial information necessary to run the business & satisfy the financial reporting requirement, e.g. the AFS
- Operating the business efficiently & effectively

Internal control is the responsibility of everyone in the business; those charged with governance of the company, management at all levels as well as ordinary employees;

- The board will have overall responsibility and accountability;
- Management will also be involved in the process of identifying risk & will be primarily responsible for designing & implementing the necessary books, records, documents, policies & procedures. Management will also be responsible for maintaining the process i.e. ensuring that policies & procedures are carried out properly & timeously & that they remain effective
- Most of the time, it is the ordinary employees who are responsible for executing the internal control procedures, e.g. signing a document, issuing a receipt, reconciling an account, and the success of the procedure will depend on them.

An efficient internal control system therefore contributes to increased certainty regarding the reasonableness of the statements in question, i.e. that **transactions** have been validly, accurately and completely accounted for. **It is therefore aimed at transactions that take place in the enterprise on a daily basis. This is in contrast to the audit objectives, which focus on transactions and balances**.

The following table, which reflects the audit objectives of transactions, events, balances and internal control objectives, should highlight the relationship between the

- **audit objectives** of **transactions, events and balances**; and
- **internal control objectives** of **transactions**.

Assertion	**Transactions and events**	**Balances: assets, liabilities & equity interest**
	X	
	Audit objective	

Occurrence	• No fictitious transactions have been recorded • All recorded transactions did in fact take place	
	Example of non-compliance • Invoice duplicated in the sales journal • Invoice prepared but goods never delivered	
Completeness	**X**	**X**
	Audit objective • There are no unrecorded transactions • All transactions that did take place & should have been included have been recorded	**Audit objective** • There are no unrecorded assets, liabilities or other balances • All assets, liabilities and balances that exist have been recorded
	Example of non-compliance • Goods delivered without an invoice being prepared • Goods delivered & invoice prepared, but invoice not recorded in the sales journal	**Example of non-compliance** • Machine in use in the factory does not appear in the fixed asset register • Debtor A's account is not included in the debtors' ledger
Accuracy	**X**	
	Audit objective • Transactions recorded at the correct numerical amounts	
	Example of non-compliance • Number of items delivered differs from the number of items that appear on the invoice • Price x quantity incorrectly calculated during the preparation of the invoice • The amount of the invoice differs from the amount recorded in the sales journal	
Cut-off	**X**	
	Audit objective • Transactions recorded on the date on which they took place	
	Example of non-compliance • Goods delivered but invoice only recorded 3 days later • Cash received a week ago only deposited & recorded today	
	X	
	Audit objective • Transactions correctly classified in the records according to their	

Classification	nature & therefore recorded in the correct account	
	Example of non-compliance - Cash sales transaction recorded as credit sales - Improvements to fixed assets recorded in the repairs account	
Existence		**X**
		Audit objective - No fictitious balances recorded - All recorded assets, liabilities & other balances do exist
		Example of non-compliance - Non-existent vehicle recorded in the fixed assets register - The debtors' list contains an amount owed by debtor X that has already been repaid in full
Rights & Obligations		**X**
		Audit objective - Recorded assets & liabilities belong to the enterprise
		Example of non-compliance - Stock held on behalf of a 3rd party appears in the records
Valuation & allocation		**X**
		Audit objective - Assets, liabilities & equity interest included at appropriate amounts & any adjustments or allocation correctly accounted for.
		Example of non-compliance - Inadequate provision for bad debts - Stock not valued at the lowest of cost price or net realizable value

The above internal control objectives could therefore be made applicable to the various applications in an enterprise, such as **the salaries & wages** application:

Internal control objective	**Objective specifically applicable to wages**
Occurrence	To ensure that wages only paid to *bona fida* employees for hours that they actually worked
Completeness	To ensure that all payroll costs are accounted for, such as deductions & amounts payable to authorities such as PAYE and UIF
Accuracy	To ensure that employees are paid for the correct hours, at the correct rates, after the correct deductions have been made from the payroll. The payroll calculation is correct
Cut-off	The ensure that payroll costs are recorded in the correct accounting period under audit, for example leave provision, bonus provision, etc.

Classification	To ensure that payroll costs are posted to the correct ledger account
Authorisation	To ensure that: • The appointment of new members of staff is authorized by management; • The termination of services is authorized by management & is properly accounted for; • Wage rates are approved by management; • Time worked (and specifically overtime) is authorized by management; • Payroll deductions are authorized

If the internal control objectives of an entity are achieved, it gives the auditor greater assurance that the assertions in the financial statements are reasonable & that the risk of material misstatement is reduced.
If the auditor has established that the entity's internal control is reliable, a reduction in the extent of substantive procedures could possibly be justified.

Control risk is defined as follows:
The risk that a misstatement that may occur in a financial statement assertion & that may be material will not be prevented or detected & timeously corrected by the **accounting and internal control systems**.

It is important that an auditor obtain an understanding of the accounting & internal control systems of an entity, and decide on the basis of an evaluation of the systems.

If the accounting & internal control systems are functioning ineffectively, the auditor would put the control risk as **high**. The opposite is true as well: if the accounting & internal control systems are functioning effectively to prevent, detect & correct material misstatements, the auditor would evaluate the control risk as **lower**.

The following schematic representation summarises the way auditors evaluate control risk:

Control risk	Reason
Low (1) ⬇	Internal controls, related to the assertion, are present which - should prevent material misstatement, or - should detect and correct it
High (2) 	Accounting system and internal controls are ineffective
High (2) 	The auditor has decided not to rely on the internal controls because it would serve no purpose, but rather to carry out extensive substantive procedures to reduce the overall audit risk to an acceptable level

(1) If the auditor has assessed the control risk as **low**, he should perform the tests of controls required to obtain audit evidence to prove that the internal controls were operating as they were designed to do during the audit period.

▪

(2) If the auditor has assessed the control risk as **high**, he should determine which errors & irregularities are likely to occur as a result of the weaknesses in the accounting system and internal controls and he should determine appropriate substantive procedures that could detect such errors.

CONTROL RISK

Control risk is a function of the effectiveness of the design & operation of internal control in achieving its objectives but because of the limitations of internal control itself, it is very unlikely that a client's system will be perfect. There are **limitations inherent to internal control**, these limitations may be described as follows:

i. management's usual requirement that the cost of an internal control does not exceed the expected benefits to be derived (cost/benefit). Control may be sacrificed due to the cost of implementing the control, thus increasing the risk that misstatement goes undetected.

▪

ii. most internal controls tend to be directed at routine transactions rather than non-routine transactions.

iii. the potential for human error due to carelessness, distraction, mistakes of judgement & the misunderstanding of instructions.

▪

iv. the possibility of circumvention of internal controls through the collusion of a member of management or an employee, with parties inside or outside the entity.

v. the possibility that a person responsible for exercising an internal control could abuse that responsibility, e.g. a member of management overriding an internal control.

vi. the possibility that procedures may become inadequate due to changes in conditions, and compliance with control procedures may deteriorate.

It is not sufficient for an auditor to simply identify the presence of weaknesses in a client's internal control system, but to evaluate the effect which the identified weaknesses may have on the financial statement assertions.

THE EVALUATION OF THE INTERNAL CONTROL SYSTEM

An auditor should obtain sufficient background information on the entity & the environment, including the entity's internal control, to enable him to identify & consider the risks of misstatement of the financial statements as a result of fraud & errors. The information the auditor obtains in this way should be sufficient to enable him to design further audit procedures. If a client has a reliable accounting system & internal controls in place, the information generated by the system will also be reliable. This implies the information will be **valid, accurate, complete and timely**.

An ineffective system could result in the financial statements not being a fair presentation of the enterprise's results.

If the auditor considers the control risk to be acceptable, he will rely on the system to produce quality information. In other words, all recorded transactions will be considered to be free of material misstatements. If the control risk is too high, the auditor would not rely on the products of the system, but only on evidence he has obtained personally.

THE TESTS OF CONTROLS

If an auditor decides to rely on the company's internal control system & has therefore provisionally rated the control risk as low, he must test the system to establish whether it is effective or not. This refers to tests of control, which are procedures carried out by the auditor to gather audit evidence on the design of the accounting and internal control systems & the operation of the systems during the reporting period.

The valuation of the auditor's findings regarding the tests of control will influence the nature, extent and timing of the substantive procedures that have to be carried out.

REPORTING

During the performance of the audit, the auditor may identify weaknesses in the internal control. The auditor evaluates the effective and continuous operation of internal controls in order to evaluate the control risk. This is one of the considerations the auditor should take into account when deciding on the nature, extent and timing of the substantive procedures.

An auditor is obliged to report on any weaknesses in the internal controls of the company of which he may become aware of during his investigation. The report should be submitted to management at an appropriate level of responsibility.

Activity:

You are a public accountant and auditor. An old friend pays a visit to your office. He has bought an existing franchise that sells motor vehicle spares. He is satisfied with the accounting & internal control systems that are in place, but he believes that there is insufficient control over cheque payments. He requests your assistance in respect of perceived weaknesses.

Design an internal control system for cheque payments that include only the most important measures for cheque payments.

1. Unused cheques should be properly controlled.
2. All cheques should be crossed.
3. People empowered to sign cheques should not have access to petty cash. They should not be permitted to approve cash payments either, or to record cash receipts or do postings to ledger accounts.
4. Only duly authorised people should be allowed to sign cheques.
5. All cheques must be signed only after they have been prepared.
6. When cheques are presented for signature, accompanying invoices & other essential evidence & documents should be presented.
7. Invoices & other supporting documents should be cancelled & the word “paid” stamped on them as soon as the cheques have been signed.
8. A bank reconciliation should be prepared at least once a month.
9. The person who prepares the bank reconciliation should not be permitted to sign cheques, to handle cash or record any cash transactions.
10. Cheques should preferably be signed by at least two independent senior officials.

Accounting systems

THE USE OF ACCOUNTING SYSTEMS

Accounting systems are used to process transactions & to keep financial records.

DEFINITION OF AN ACCOUNTING SYSTEM

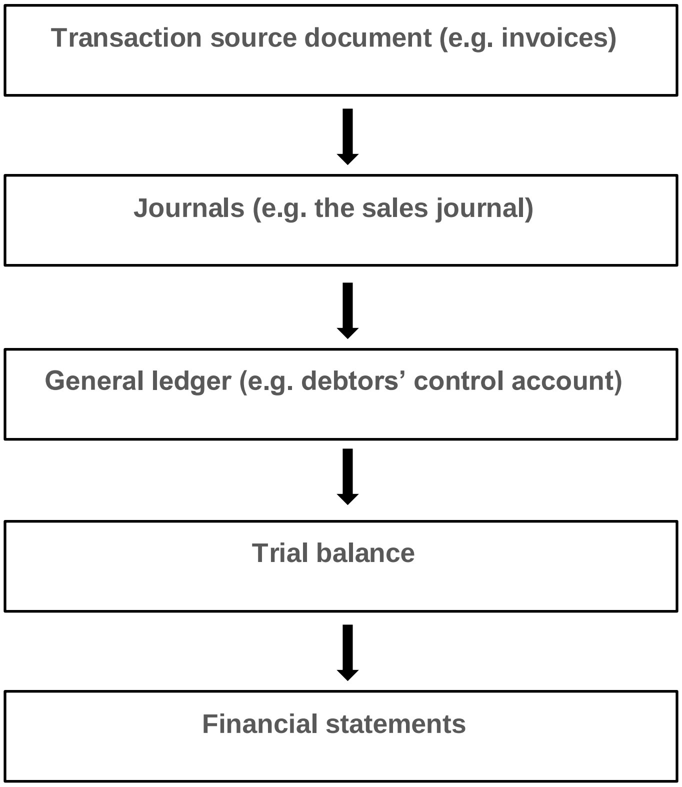
An accounting system is defined as the functions by means of which an entity's transactions are processed in order to maintain accounting records.

THE NATURE OF ACCOUNTING SYSTEMS

Every company shall keep in one of the official languages of the Republic such accounting records as are necessary to fairly present the state of affairs & the business of the company and to explain the transactions & financial position of the trade or business of the company.

The Companies Act states that it is the duty of the auditor of a company to satisfy himself that **proper accounting records** as required by this Act have been kept.

An **accounting system** is the basis for the creation of **accounting records** since it is the accounting system that identifies transactions, assembles and analyses transactions, summarises the information & generates reports. The flow of transactions in an accounting system can be represented as follows:


Transaction source document (e.g. invoices)
Journals (e.g. the sales journal)
General ledger (e.g. debtors' control account)
Trial balance
Financial statements

An accounting system focuses on transactions that include the exchange of assets & services between a business enterprise & third parties, as well as the transfer or use of services within the company.

Accounting systems should also provide a complete transaction or audit trail for every transaction. A transaction or audit trail, which is required by both management & the auditors, may be defined as follows:

- It is a chain of evidence that is created by coding, cross reference & documentation and that links account balances & other summary results to the original transaction data.

An <u>effective</u> accounting system = Accounting system + Internal controls

The following example can be used to explain the above:
The management of Piet Limited has implemented an accounting system in terms of which Mr P records all individual sales transactions on an invoice. These invoices are recorded in the sales journal on a daily basis. Mr Q is responsible for updating the general ledger on a monthly basis. Mr B uses the ledgers to prepare annual financial statements for submission to the auditors.

If management does not implement the additional control procedures, such as issuing invoices in numerical sequence and checking on any missing numbers on a monthly basis, then it is clear that although an accounting system may be applied, that the system is **not** sufficient on its own to ensure that all financial information has been completely recorded.

An effective accounting system should therefore:

1. identify and record all valid transactions.
2. describe the transactions in sufficient detail on a timely basis to permit proper classification of transactions for financial reporting.
3. measure the value of transactions in a manner that permits recording their monetary value accurately in the financial statements.
4. determine the time period in which transactions occurred to permit recording of transactions in the proper accounting period.
5. properly present the transactions and related disclosures in the financial statements.

RESPONSIBILITY FOR THE DESIGN, IMPLEMENTATION AND MAINTENANCE OF ACCOUNTING SYSTEMS

An accounting system is a series or collection of tasks & records by which transactions are processed to create financial records. An accounting system identifies, assembles, analyses, calculates, classifies, records, summarises and reports transactions & other events. The major elements of the accounting system are **people** who carry out **procedures** e.g write out a credit sales invoice, calculate a price, enter the invoice in a sales journal, etc, and **paper** such as order forms, ledgers, lists, invoices etc, which facilitate the initiation, execution and recording of the transaction.

Management must now add **control activities (actions)** to the accounting system if it is to produce financial information which is representative of transactions which have occurred and were authorized and which is accurate and complete and which is timeously produced. Management now adds **control activities**; before the invoice is written out, the salesperson checks that the customer is a valid account holder & that the customer is not behind on his payments and will not be exceeding his credit limits; a second salesperson may check the invoice to ensure that pricing, discounts and VAT calculations are correct. At a later stage, an accounts clerk may confirm that all invoices for the week have been entered into the sales journal.

The responsibility for the prevention and detection of errors and fraud rests with the management and the persons who are responsible for the corporate governance of an organization. How do you think management accomplishes this task?

* by maintaining a suitable accounting system;
* by designing and implementing appropriate internal controls to maintain the reliability & integrity of the accounting system.

ASPECTS OF IMPORTANCE IN THE DESIGN OF ACCOUNTING SYSTEMS

The **management** is responsible for the design of an accounting system. The following aspects should be taken into account by management when designing an accounting system:

- the requirements of the Companies Act, the Standards and any relevant legislation;
- aspects of internal control;
- the availability of technology to determine the type of accounting system (manual or electronic)

DATA PROCESSING METHODS

Data processing methods have changed to keep pace with changes in technology. Accounting systems originally relied on manual methods, then they were carried out mechanically and ultimately they relied on electronic means.

The various processing methods, with a definition of each, and a description of their influence on the auditor's tests, are shown in the following table:

Data processing method	Description of data processing method	Influence of data processing method on the auditor
Manual systems 	In a manual system the following procedures are done manually: - the posting of source documents to the appropriate journals - the posting of totals from the respective journals to the general ledger - the preparation of a trial balance from the general ledger - the preparation of reports from the general ledger or the trial balance	When performing his tests, the auditor can ***visually*** inspect the documents, journals, ledgers, trial balances and reports.
Mechanical systems 	Mechanical systems utilize data processing equipment such as unit record equipment. This equipment processes all transactions, journals & ledgers that appear on punch cards. For example: - To update an account, an account card showing the previous balance is read. A transaction card is then read. A new account card showing the updated balance is then printed. - Reports are prepared by reading & printing the amounts on the updated account balance cards.	Since data processing equipment is involved, auditors have to understand machine control in order to establish whether debits and credits have been correctly posted. The tracing and visual inspection of transactions is possible with a mechanical system, but it makes the auditor's task more difficult. With unit record equipment the tracing of transactions can still take place, but the auditor must be able to read punch cards. Visual inspection is more difficult as a result of the speed at which data processing equipment processes the punch cards.
Electronic data processing systems (EDP) 	Computers are used for transaction processing. This processing can take place in one of the following ways: - Individual transactions are immediately processed (real time).	The auditing of such a system is far more complex. Since the processing of transactions takes place electronically, it is difficult for the auditor to trace a transaction visually from a source document to a journal, ledger, trial balance and ultimately a report. The auditor therefore has to develop other

	- Accumulated batches of transactions are processed periodically.	procedures & techniques in order to carry out audit tests effectively.

Activity:

What are the characteristics of an effective accounting system?

An effective accounting system should:

1. Identify and record all valid transactions
2. Describe the transactions in sufficient detail on a timely basis to permit proper classification of transactions for financial reporting.
3. Measure the value of transactions in a manner that ensures that their proper monetary value will be recorded in the financial statements.
4. Determine the time period in which transactions occurred to ensure the recording of transactions in the proper accounting period.
5. Ensure that transactions are properly accounted for and disclosed in the financial statements.

Study Unit 2.4

Internal control systems

THE PLACE OF INTERNAL CONTROL IN THE MANAGEMENT OF AN ENTITY (BUSINESS)

The purpose of internal controls is to address the risk of something undesirable, unintended or illegal, from occurring.

In a business, management is responsible for running all aspects of the entity. The objectives of the business will be set, the risks relating to achieving those objectives will be identified and suitable books, records and documents, and policies and procedures will be put in place to address those risks. This will include addressing the risks associated with such matters as:

- Safeguarding the assets of the company, e.g. inventory, from theft or damage;
- Preventing fraud;
- Complying with the laws and regulations applicable to the entity;
- Producing reliable financial information necessary to run the business and satisfy the financial reporting requirements, e.g. the AFS
- Operating the business efficiently and effectively.

WHAT HAVE WE LEARNT ABOUT INTERNAL CONTROL?

1. **Internal control is a process**. It is a combination of systems, policies and procedures designed, implemented & maintained to address the risks of running a business.

2. **Internal control is affected by people**. It does not consist solely of policy and procedure manuals, ledgers and documents, computers and machines; it involves people at every level of the organization carrying out an assortment of tasks.

3. **Internal control is not the sole responsibility of management**. There is a share responsibility for the internal control process; the directors' management and ordinary employees are all, in their own ways, responsible.

4. **Internal control is not static**. It is essentially a response to the risks of operating a business; risks change, responses must change.

5. **Internal control is not foolproof**. It provides only reasonable assurance that the risks that threaten the objectives of the business will be achieved.

6. **Internal control is not a case of a single control addressing a single risk**. Internal control policies & procedures must work in conjunction with each other & with the books, records and documents used. The control over a risk is best achieved by combinations of actions, policies & procedures.

It is the task of management, and not the auditor, to design and implement effective internal control systems in order to manage the enterprise's risks and ensure that attention is paid to all aspects of control.

This means that management is responsible for the preparation of financial statements in accordance with generally accepted accounting principles (GAAP). The preparation of financial statements is not the auditor's task.

DEFINITION OF AN INTERNAL CONTROL SYSTEM

Internal control can be defined 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:

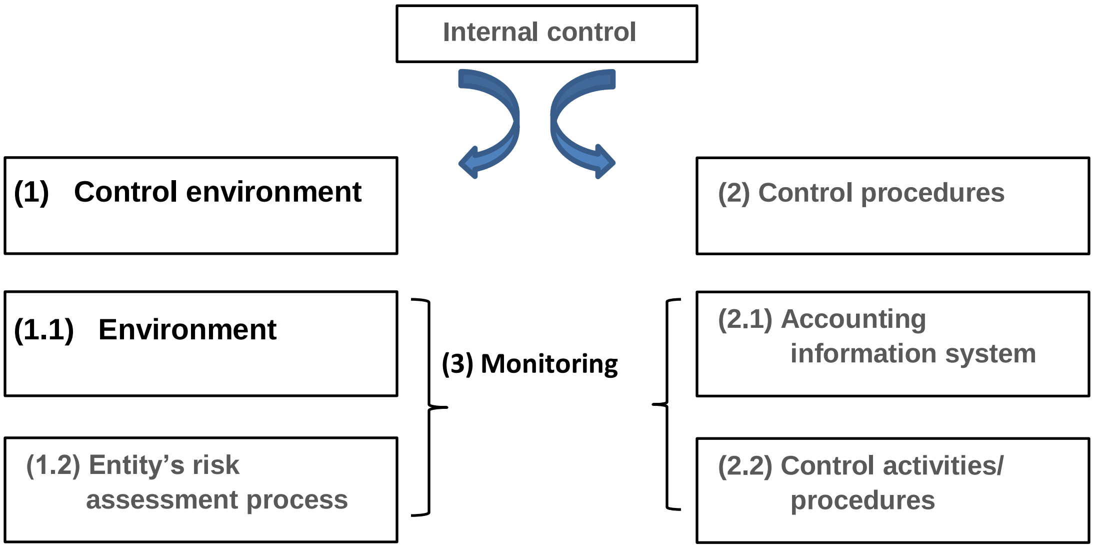
- the reliability of the entity's financial reporting;
- the effectiveness and efficiency of its operations; and
- its compliance with applicable laws and regulations

THE EXTERNAL AUDITOR'S INTEREST IN INTERNAL CONTROL

The external auditor is primarily interested in the fair presentation of the entities annual financial statements. The financial statements are a product of the entity's information systems which includes the accounting system. The better the internal control process, the more likely the financial statements are to fairly present.

ISA 315 – Identifying and assessing the risks of material misstatement through understanding the entity & its environment, requires that the auditor obtain an understanding of the entity's internal control & suggests that a good way of doing this may be to evaluate the five components of internal control. An understanding of the information systems and control activities are equally important for the auditor as, without understanding these, the auditor is unable to properly assess the risk that management's objective of producing valid, accurate and complete financial information will be achieved.

COMPONENTS OF INTERNAL CONTROL


Internal control
(1) Control environment
(2) Control procedures
(1.1) Environment
(3) Monitoring
(2.1) Accounting information system
(1.2) Entity's risk assessment process
(2.2) Control activities/ procedures

COMPONENT		DEFINITION
Control environment	• integrity & ethical values • commitment to competence • participation of those charged with governance • management's philosophy & operating style • organizational structure • assigning authority & responsibility • human resource policies & practices	The **attitude, awareness & actions** of owners, directors & management in respect of the importance of the internal control system. This sets the **tone** in the organization – it influences the employees' awareness. This is the **foundation** for all other **control components**.
Risk assessment	• define the objectives of the entity, its departments &functions • identify & assess risks - operational risks - financial reporting risks - compliance risks • respond to risk - information system - control activities	The process management follows in **identifying**, **analyzing and responding to risks** that are relevant to the preparation of financial statements that are a reasonable reflection of the financial position and results of the operations and cash flow of the entity. This forms the **basis** for the determination of **control activities**.
Accounting information system	• valid, accurate & complete • procedures to deal with transactions - initiating - recording - processing - correcting - posting (to ledgers) • related accounting records - documents used - document design • capturing events & conditions other than transactions • journal entries	This comprises the functions (computerized and manual) by means of which the entity gathers, processes and accounts for information.
Control activities / procedures	• actions, procedures supported by policies - approval, authorisation - segregation of duties	These comprise techniques, methods and principles that are necessary for the application of internal control. These are the

	- isolation of responsibility - access/custody (security) - comparison & reconciliation - performance reviews • preventive, detective • general & application	policy measures and procedures that the management has instituted in response to internal and external risks.
Monitoring	• assessment over time • are objectives being met? • Assessment at all levels - directors - management - department heads • independent assessment - internal audit - external bodies - customers • remedial action	Management should consider on a regular basis whether the control measures are functioning as they were intended to do, for example **management supervision and oversight**.

Component 1: *the control environment*

A good control environment will be characterised by:

- communication & enforcement of integrity & ethical values throughout the organization;

▪

- a commitment by management to competent performance throughout the organization;

▪

- a positive influence by those charged with governance (are they independent, do they display integrity and ethical commitment, and are their actions & decisions appropriate?);

▪

- a management philosophy & operating style which encompasses leadership, sound judgment, ethical behavior, etc.;

▪

- an organisational structure which provides a clear framework within which proper planning, execution, control and review can take place;

▪

- policies, procedures and an organizational structure which clearly define authority, responsibility and reporting relationships throughout the entity;

▪

- sound human resource policies and practices which result in the employment of competent ethical staff, provide training and development as well as fair compensation and benefits, promotion opportunities, etc.

▪

Gathering of evidence relating to the control environment can be achieved by ***observation*** of management and employees “in action”, including how they interact, ***inquiry*** of management and employees, e.g. union officials, and ***inspection*** of documents, e.g. codes of conduct, organograms, staff communications, records of dismissals, etc.

Component 2: *the entity's risk assessment process*

This is the process which the company has in place for, i.e.:

- identifying business risks relevant to financial reporting objectives;
- estimating the significance of each risk;
- assessing the likelihood of its occurrence;
- responding to the risk

Information about the client's risk assessment process will be gathered mainly by ***inquiry***, e.g. Risk Officer, Compliance Officer, and ***inspection*** of documentation where it is available, e.g. minutes of designated committee meetings, inter-office memo's.

Component 3: *the information system*

The auditor is required to obtain an understanding of the information system relevant to financial reporting & communication. The accounting system is part of the information system. The auditor must obtain a thorough understanding of:

➢ the classes of transactions in the client's operations that are significant to the financial statements, e.g. sales, wages

▪

➢ the procedures within both IT and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements

▪

➢ the related accounting records, supporting information & specific accounts in the financial statements in respect of initiating, recording, processing and reporting transactions

▪

➢ how the information system captures events & conditions, other than transactions that are significant to the financial statements, e.g. contingent liabilities

▪

➢ the financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures

▪

➢ controls over the passing of non-standard journal entries used to record non-recurring, unusual transactions or adjusments

▪

➢ the manner in which financial information is conveyed to management , the Board, the audit committee & external bodies, e.g. the JSE in the case of a listed company

▪

The chart below provides a breakdown of matters which the auditor might consider when obtaining information about a ***computerised*** information system.

FACTOR	MATTERS TO CONSIDER
Computerised applications	a) which applications are computerized, e.g. • payroll – not computerized

	• acquisitions and payments – computerized b) computer environment • micro, network, centralized • use of bureau c) the application software • purchased or in-house software • key processing functions • nature and source of inputs • output produced • important materfiles and tables • interface between applications • new or established
Hardware	a) makes and capacities of CPU's, drives, printers, servers, terminals (important for establishing compatibility with the auditors hardware & software and for understanding the system) b) physical location (branches, factory, etc)
Software	a) details of all software which is used for managing the functions of the hardware and data • operating systems • database management systems • utilities • access control software • programme change control software
Organisation and control	a) general and application controls b) communication and reporting lines c) IT personnel and their job descriptions d) steering committee details e) internal audit involvements in IT
Complexities of the system	a) the presence of: • networks (LANS, WANS) • electronic data interchange (EDI) • electronic funds transfer (EFT) • real time systems • the Internet • high levels of system integration • complex databases, communication networks
The level of dependence (of the client on its normal system)	a) degree of disruption which would occur if the system was not functional for a lengthy period b) the dependence of a particular functional area on timely, accurate computing, e.g. wages in a large labour intensive industry

The auditor should be mindful that **computerized (IT) systems pose specific risks** to an entity's internal control. These risks include the following:

a) A computer will process what is input and will do so in the manner in which it is programmed. If for example there is an error in programming, that error will be repeated every time the relevant transaction is processed, e.g. a programming error results in the VAT on sales being calculated on the selling price plus VAT e.g. 14% of 114%. If 5000 invoices are processed the computer will make the mistake 5000 times.

▪

b) Unauthorised access to data can result in instant and huge destruction or contamination of data e.g. deletion of the debtors masterfile.

▪

c) IT personnel gaining access privileges they should not have, resulting in a breakdown of segregation of duties e.g. a systems analyst gains access to the salaries masterfile & alters his salary.

▪

d) Unauthorised changes to data in masterfiles, systems or programmes.

▪

e) Processing of fraudulent transactions instantaneously e.g. unauthorised funds transfer which almost instantaneously moves money out of the company's bank account.

▪

f) Potential denial of access to electronic data e.g. can't get into the database because of system failure.

▪

The auditor should also be mindful that the information system as a whole, or part thereof, can be placed at risk, by for example:

a) **New employees** who have a different understanding of, or attitude to internal control;
b) **Rapid growth** in the company which places severe strain on the controls;
c) **New technology** which can lead to disruption of internal controls;
d) **Introducing new business models** which may result in the existing internal controls being rendered inadequate;
e) **Corporate restructuring** which may result in staff reductions, new lines of authority, etc., thereby jeopardizing for example, division of duties and authorisation controls.

Details of the information system (including the accounting system) can be gathered by:

1. **Inspection** (or creation) of flowcharts of the system
2. **Observation** of the system in action, e.g. what happens when goods are delivered by a supplier
3. **Inquiry** of client staff & the completion of internal control questionnaires
4. **Discussions** with prior year audit staff, management & possibly outsiders, e.g. application software suppliers
5. **Discussions** with internal audit staff & **review** of internal audit workpapers
6. **Tracing** transactions through the information system, sometimes called "walk through" tests

Component 4: *control activities*

Control activities are the policies and procedures that are implemented to ensure that management's objectives are carried out. Control activities essentially include such things as:

- authorisation of transactions (which is a form of isolating responsibility);
- segregation of duties, e.g. separating custody of inventory from keeping of inventory records;
- physical control over assets, e.g. restricting access to the warehouse;
- comparison and reconciliation, e.g. reconciling the bank account monthly;

- access controls, e.g. access tables, user profiles, Ids and passwords in a computerized environment;
- custody controls over blank / unused documents, e.g. cheque books, order forms;
- good document design (to achieve accuracy & completeness of information);
- sound general and application controls in IT systems

Component 5: ***monitoring of controls***

Monitoring of the system tells management how well the internal control process is doing. Management (and the Board) wish to know if controls are operating as intended and monitoring assists in providing this information.

Information about monitoring can be obtained by the auditor by **inquiry** of management and staff working with internal audit and **inspecting** documentation relating to a monitoring process or performance reviews.

INHERENT LIMITATIONS OF INTERNAL CONTROLS

LIMITATION	REASON FOR EXISTENCE
1) Cost of internal control	A control may be inefficient because the cost of implementing it exceeds any benefit that could be derived from it
2) Human error	Generally arises from carelessness, interruptions, bad judgement on the part of an employee or misunderstanding of instructions
3) Problems with non-routine transactions	Internal controls are usually designed to deal with routine transactions
4) Collusion	A person (or more than one person) could be in collusion with parties inside or outside the entity to circumvent certain internal controls
5) Controls may become inadequate	Controls may become inadequate because conditions change continually, the internal controls are not always adjusted accordingly and compliance with procedures sometimes becomes lax over time
6) Abuse of responsibility	A responsible officer could abuse his position

INTERNAL CONTROLS PRINCIPLES (CHARACTERISTICS OF GOOD INTERNAL CONTROL)

The auditor focuses mainly on those aspects that ensure that valid, accurate and complete financial information is provided.

To be able to evaluate internal controls and make recommendations on possible weaknesses in and improvements to internal control systems, the auditor requires a thorough knowledge of control activities.

Management institutes internal controls on the basis of these principles of internal control.

The auditor is not responsible for the internal controls of an enterprise. His task is to evaluate the effectiveness of the controls to determine the appropriate nature, extent and timing of substantive procedures.

Activity:

ABC Stores is a general dealer with branches throughout South Africa. Their head office is in Johannesburg. Once a month the branches receive inventory from head office. The branches are only permitted to buy inventory for cash.

One of the aspects of control activities is proper control over the storage of inventory. To verify that proper control over the storage of inventory is being carried out, the auditor must make certain that adequate physical security measures and access controls are in place for all the assets of the enterprise.

Required:

Describe the internal controls that would ensure that proper control over the storage of inventory and assets is exercised at all the branches of ABC Stores.

Feedback:

1. Management should prohibit any unauthorized access to the premises and buildings.
2. An appointed person should be given responsibility for authorizing access to fixed and other assets of the entity.
3. Lockable storage facilities should be available and somebody should be appointed to exercise adequate control over the keys.
4. If goods have to be delivered, there should be only one exit from the business premises, and that exit should be guarded by gate guards so that no goods can leave the premises without the necessary delivery note / invoice.
5. If goods are sold directly to the public, there should be adequate controls over the use of cash registers. The number of exits should be limited, and security staff should make certain that customers have paid for the goods that leave the premises.
6. Customers should not have direct access to items with a high value.
7. Large sums of cash should never be kept in cash registers. Cash should be removed regularly by a responsible person and deposited.
8. Cash that is not banked in time should be locked up in a safe until it can be banked.
9. An appointed person should regularly compare the financial records and physical assets (fixed and other assets). Explanations should be sought for any shortfalls and deviations.

Concepts in computer information systems (CISs)

THE COMPONENTS OF INTERNAL CONTROL AND INFORMATION TECHNOLOGY SYSTEMS (IT)

Internal controls can be defined 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

In terms of ISA 315, the auditor is required to gain an understanding of the company's internal control system and this understanding can be best obtained by considering the 5 components of internal control. These components are:

1) the control environment;
2) the company's risk assessment procedures;
3) the information system, including relating business processes relevant to financial reporting;
4) control activities;
5) monitoring of controls

When considering each component, the auditor will need to consider the effect of the company's IT (computerization) on that component.

1) THE CONTROL ENVIRONMENT

This is about management's attitude to and awareness of the need for controls. Because of the potential major consequences of poor control in a computerized system, a strong control environment is very important. The evaluation of the control environment will be far more intense in a large, highly computerized company (bank) than in a smaller business.

2) THE COMPANY'S RISK ASSESSMENT PROCEDURES

The King III report on corporate governance recognizes information technology (IT) risk as one of the major risks facing a company. Whilst managing IT risk is the responsibility of the board, it is likely that the board will delegate its responsibility to a risk committee. The IT structure may include a steering committee and a chief information officer. Part of this internal control component's function will be to focus on the assessment of (and response to) the IT risks facing the company e.g. data security and privacy, business continuity, data recovery and keeping up with technology, etc.

3) THE INFORMATION SYSTEM, INCLUDING BUSINESS PROCESSES RELEVANT TO FINANCIAL REPORTING

The information system is described (by ISA 315) as "consisting of infrastructure (physical and hardware components) software, people, procedures and data. When the auditor is gathering information about this component he will need to familiarize himself with each of the above and how they interact. ISA

315 also explains that the information system relevant to financial reporting objectives, which includes the accounting system, consists of the procedures and records designed and established to:

- initiate, record, process and report entity transactions, events and conditions and to maintain accountability for the related assets, liabilities and equity;
- resolve incorrect processing of transactions;
- process and account for system overrides, e.g. by the creation of audit trails in the form of a log of overrides;
- transfer information from transaction processing systems to the general ledger e.g. where the revenue application software is not integrated with the general ledger, a journal entry will have to be passed to get sales and debtors totals into the general ledger;
- capture information other than transactions, such as depreciation and allowances for bad debts;
- ensure information required for disclosure is accumulated, recorded, processed, summarized and appropriately reported in the financial statements;
- authorise and process journal entries
-
-

4) **CONTROL ACTIVITIES**

This is the component of internal control which will probably interest the auditor the most because these control activities (policies and procedures) have a big influence on whether the financial information records and processes only authorized transactions which are authorized and have already actually occurred, and has done so accurately and completely.

It is important to remember that control activities in a computerized system will be a combination of manual and automated (programmed) controls.

5) **MONITORING OF CONTROLS**

This component concerns management's responsibility to assess whether the internal control system is meeting its objectives over time. It is not just about monitoring whether the control activities are taking place, it is also about assessing whether they are affective. Monitoring is also not about assessing control activities; it is also about evaluating the other components of the internal control system, e.g. the control environment and the risk assessment process. In a computerised environment the amount and variety of information which can be quickly and accurately obtained from the system enhances the ability of management, those charged with governance as well as various bodies such as the internal audit department as well as audit and risk committees, to conduct effective monitoring over time.

DIFFERENT TYPES OF COMPUTER SYSTEMS

The following table describes and illustrates the different types of computer systems with reference to examples.

Computer system	Definition	Example
Online input with real-time processing	Transactions are captured at a terminal, automatically authorized & the computer files are updated immediately. As a result, the transaction & masterfiles are immediately up to date.	If someone books an air ticket, the seats available masterfile for the flight in question is captured online and immediately processed. Can you see the necessity for this processing method in the given example? If the masterfile is not updated in real time, there is a risk that a seat could be booked more than once.
Online input with batch processing	Transactions are captured via a terminal, authorized and written to a transaction file. The transactions are added to the masterfiles later. The result of this is that the masterfiles are not updated immediately.	Orders for hair products are placed by the public. An input operator inputs the orders on a terminal as soon as the order form has been received. The order forms are written to a separate transaction file. Later on the order forms on the transaction file are processed to the masterfile in a batch.
Batch input with batch processing	Data are captured manually on purpose-generated source documents. The source documents are then assembled in batches (the number of source documents per batch is determined in advance). They are then inputted into the computer in a computer-readable format, after which they are stored	Time cards are updated daily by 100 factory workers. At the end of the week the time cards are submitted to the factory foreman. They are then sent to the input operator, who makes up the time cards into batches of 20. The time cards are sequentially read into the computer by the input

	on the computer system in a transaction file. At a given time the relevant masterfile is updated with the new data from the transaction files.	operator and each batch is stored in a transaction file on the computer system. Two days before the payment of wages, the payroll masterfile is updated from the various transaction files.

CONTROL TECHNIQUES AND APPLICATION CONTROLS

1.1 Batch entry, batch processing / update

- ➢ Transaction data is captured initially onto manually prepared source documents e.g. sales invoices.
- ➢ These source documents are then collected into batches usually after manual checks have been performed and entered via the keyboard with control totals in these batches. Relevant programme checks take place as the information is keyed in e.g. validation check on employee number. The transaction information is converted into machine readable form and held on a transactions file on the computer system.
- ➢ These transactions are then processed as a batch when it is efficient / convenient to do so and the relevant masterfiles are updated to reflect the effect of the entire batch on affected masterfile balances. Control totals before and after processing are compared.
- ➢ Not common, particularly as it is slow and information is not up to date.

1.2 On-line entry, batch processing / update (also referred to as on line entry with delayed processing)

- ➢ Transaction data is entered, via a keyboard immediately as each transactions occurs e.g. a sales order is placed by telephone and the operator keys in the details as the conversation with the customer takes place. Relevant programme checks take place as information is keyed in (for simplicity sake, assume an invoice is created immediately and not only after goods have been dispatched).
- ➢ The transaction information is converted into machine readable form as each transaction occurs and is held on a transactions file on the computer system.
- ➢ Control totals are created by the computer on the batch for the transaction file.
- ➢ The transactions are then processed as a batch and the relevant masterfiles are updated to reflect the effect of each transaction in the batch on affected masterfile balances, e.g. they could be processed at the end of each day (daily batch update).
- ➢ Entry of the transaction is efficient, but information is not immediately up to date. The longer the period that the batch of transactions is not processed, the less up to date the information.

1.3 On-line entry, real-time processing / updated

- ➢ Transaction data is entered, via a keyboard, immediately as each transaction occurs. Relevant programme checks take place as information is keyed in.
- ➢ The relevant masterfiles are also updated immediately to reflect the effect of each individual transaction on affected masterfile balances, e.g. a seat booked on an air craft will instantly update the "seats available masterfile" which is really an inventory masterfile, for that particular flight. Obviously this could not be done in batch mode as the same seat could be booked numerous times before the masterfile is updated.
- ➢ Entry of the transaction is efficient (access controls are very important) and information is right up to date.

CIS INTERNAL CONTROLS (CATEGORIES)

Internal control in a computer environment is achieved by implementing and maintaining general controls and application controls (each category probably consists of user (manual) and programmed (computerised) controls.

The object of such controls is to ensure that:

a) the computer system is properly developed, implemented and maintained (**general controls**);
b) proper controls are in place to ensure the validity, completeness and accuracy of transactions and data (**application controls**)

Certain controls fall under both general and application controls. Access controls apply to both categories, as illustrated below.

- ★ **General controls**: to control access to data and programs
- ★ **Application controls**: to control access to specific program functions to ensure the validity of input, processing and output.

ELEMENTS OF A COMPUTERISED DATA PROCESSING SYSTEM

The following are the elements of a data processing system:

- hardware
- systems software
- application software
- procedures
- staff

HARDWARE

The term “hardware” collectively describes all the equipment necessary to perform a data processing function. This equipment includes the following:

Central processing unit (CPU)	This consists of the primary storage unit where the output of the computer is stored, the mathematical unit which performs the calculations and the control unit which controls functions such as the keyboard.
Input devices	These consist of the keyboard, the disk drives & the scanners. For example, the prices of items at a supermarket are read from the barcodes by means of a scanner.
Output devices	These consist of the printer and the computer screen.
Data preparation equipment	Such equipment is used for an offline function, in other words the function can be performed while the device is not linked to the computer. For example, batch information (time cards) can be read in, converted to computer language, and then stored on a compact disk (CD). The CD is later used to read the time card information into the computer.

SYSTEMS SOFTWARE

Systems software is a set of programs (instructions) that coordinate the use of the hardware & supports the running of computer programs. It includes the following:

Operating system	Examples of operating systems are Windows or DOS
Database management system (DBMS)	This is the program used to create & store the data & manage the database. Along with the operating system, the DBMS facilitates the storage of data, defines the relationships between data and makes data available for use by the application programs.

APPLICATION SOFTWARE

Application software refers to programs designed to meet specific data processing needs, such as the processing of wages and creditors.

PROCEDURES

Even if the computer hardware & software works automatically, it is still necessary for personnel to follow proper procedures to operate the computer effectively. These procedures relate to data preparation, the use of the computer, etc.

PERSONNEL

To get an electronic data processing system working properly requires personnel with sufficient training & experience to perform the various specialised tasks.

Activity:

Credit sales transactions are recorded by means of a manual system, as described below:

A sales invoice is made out by hand in triplicate by the sales clerk. At the end of the day the debtors’ ledger & the sales and inventory records are updated from copies of the sales invoices.

Briefly indicate how the above transaction would be recorded if the transaction were processed by each of the following kinds of computer systems:

(1) batch input/batch processing
(2) online input/batch processing
(3) online input/real-time processing

Feedback:

(1) Batch input/batch processing

- A credit sales invoice is made out by hand in triplicate by the sales clerk.
- At the end of the day the invoices are batched & captured on computer.
- After the input of the batch invoices, the batch is processed by the computer & the debtors' file and the sales and inventory records are updated.

(2) Online input/batch processing

- A credit sales transaction is captured directly on the computer by the sales clerk & is then stored by the computer.
- A sales invoice is prepared and printed by the computer.
- At the end of the day the whole day's credit sales transcations are processed by the computer and the debtors' file and sales and inventory records are updated.

(3) Online input/real-time processing

- A credit sales transaction is captured directly on the computer by the sales clerk.
- The transaction is immediately processed by the computer and the debtors' file and sales and inventory records are then updated.
- The computer then prints the sales invoice immediately.

Corporate governance

KING III – CODE OF GOVERNANCE PRINCIPLES (effective March 2010)

The primary reasons for King III were:
- The promulgation of the Companies Act 2008 and
- Changes in international trends

The King III Code identifies two bases as "comply or else" or "comply or explain" and describes a variation of the latter, i.e. "apply or explain".

- ★ "**comply or else**" conveys that companies must adhere to the rules and if they don't, they will be punished.
- ★ "**comply or explain**" conveys that the principles and practices recommended by the Code should be the focus of the company's corporate governance. However, if the directors consider that compliance with a particular recommendation is not in the best interests of the company then the directors are at liberty not to comply but must explain the reason behind their decision.
- ★ "**apply or explain**". The word "comply" is too strong and inflexible. Using the word "apply" suggests a more accommodating approach. Thus King III is on the "apply or explain" basis.

"APPLY OR EXPLAIN" AND THE LAW

The "apply or explain" basis does not mean that corporate governance and the law can be separated. As the term suggests, corporate governance is about governing companies. This is achieved by the directors of the company putting in structures, processes and procedures which achieve the objectives of the company but within the framework of the law. The directors themselves have legal duties:

- ❖ They are obliged to act with a duty of care, skill and diligence in managing the business; and
- ❖ They have a fiduciary duty to act in the best interests of the company, to avoid conflicts, and not to make secret profits.
- ▪

If they fail in these fundamental duties they can be found guilty of gross negligence, misconduct or breach of trust.

The Companies Act 2008 requires that public companies & state owned enterprises be audited and that they appoint audit committees. In fulfilling their duties, the directors must ensure that this happens.

The Act also makes certain individuals ineligible for appointment as a director such as a person convicted & imprisoned for theft, forgery or fraud; directors must declare their financial interest in any matter to be considered at a meeting of the board and as a final example, directors must produce financial statements to stakeholders. These legal requirements, all related to governance, must be complied with.

KEY ASPECTS OF THE KING III REPORT

a) **Leadership** – good governance is about effective leadership. Leadership is characterized by the ethical values of responsibility, accountability, fairness and transparency & is based on moral duties that find expression in the concept of Ubuntu (humaneness, mutual support and respect, interdependence, unity, collective work and responsibility).

▪

b) **Sustainability** – companies are part and parcel of society and must address, and be part of the social, ethical and environmental issues which arise out of society. Should a company fail to understand and react to its position in society, the implication is that it will not survive i.e. it is not **sustainable**. There is no sustainability or future for companies which ravage the environment or exploit their constituency.

▪

c) Corporate citizenship – the concept of corporate citizenship flows from the fact that the company is a person and should operate in a sustainable manner. Companies have rights but also legal and moral obligations in respect of their economic, social and natural environments.

SUSTAINABILITY

The important aspects of sustainability are:

1. **Inclusivity of stakeholders**: to achieve sustainability, the legitimate interests and expectations of **all** stakeholders must be taken into account in decision making and strategy. Stakeholders will include, employees, suppliers, the community in which the company operates, investors, customers, etc.

▪

2. **Innovation, fairness and collaboration**: these are key aspects in achieving sustainability. Innovation provides new ways of achieving sustainability, fairness is vital because social injustice is unsustainable and collaboration (and co-operation) is required if business at large is going to embrace the principles of sound corporate governance proposed by King III.

▪

3. **Social transformation**: to achieve sustainability, social transformation must be part and parcel of a company's performance.

▪

IMPORTANT ISSUES INCORPORATED INTO THE KING III REPORT

1. **Alternative dispute resolution (ADR)** – where disputes arise in business dealings, mediation/arbitration as opposed to going to court is an acceptable way of resolving the dispute. From a governance perspective, where a dispute arises, it is a duty of the directors to resolve the dispute timeously, efficiently and effectively. ADR clauses are now frequently included in contracts and mediation and arbitration should be regarded as "good governance".

▪

2. **Risk-based internal audit** – King III favours risk based internal audit over compliance based internal audit. The compliance based approach has internal audit checking that the company has complied with its internal controls, legislation, etc. The risk-based approach places more emphasis on internal audit understanding the risks associated with the strategic direction of the company and determining whether internal controls, processes and procedures, adequately address these risks.

▪

3. **IT governance** – if you think about the international banking system, electronic banking, use of the internet by businesses, it is very easy to understand that issues such as confidentiality, integrity, functionality of the system are of paramount importance in the management of the company.
    -

4. **Business rescue** – rescuing a business means that the business has been sustained, and is clearly in the interests of all the business's stakeholders.
    -

APPLICATION OF THE CODE

King III applies to all entities regardless of the manner and form of incorporation. The size and nature of the company will determine how the entity applies the recommendations, and it is recommended by King III that all entities disclose which principles and / or practices they have decided not to apply and explain why.

The King Code of Corporate Governance (King III) deals with the following aspects:

- Ethical leadership and corporate citizenship
- Boards and directors
- Audit committees
- The governance of risk
- The governance of information technology
- Compliance with laws, rules, codes and standards
- Internal audit
- Governing stakeholder relationships
- Integrated reporting and disclosure

ETHICAL LEADERSHIP AND CORPORATE CITIZENSHIP

Principle 1.1: The board should provide effective leadership based on an ethical foundation
Principle 1.2: The board should ensure that the company is, and is seen to be, a responsible corporate citizen
Principle 1.3: the board should ensure that the company's ethics are managed effectively

Principle 1.1: **The board should provide effective leadership based on an ethical foundation**

a) The company's strategy must take into account the economy, society and the environment.
b) The board is answerable to all of the stakeholders of the company.
c) All aspects of corporate governance are based on ethical values and standards, and the ethics of governance require that all decisions and actions of the board be based on four ethical values:

- ★ **Responsibility** – the board should assume responsibility for the assets and actions of the company and should take corrective action to keep the company on its correct path.
- ★ **Accountability** – the board should be able to justify its decisions and actions to all stakeholders.

- ★ **Fairness** – in its decisions and actions, the board should ensure it gives fair consideration to the interests of all stakeholders.
- ■
- ★ **Transparency** – the board should disclose information in a manner that enables all stakeholders to make informed analysis of the company's performance.

■

With regard to a director, the ethics of governance require that each director adhere to these **five** basic ethical values and that each director exercise the following moral duties:

1. **Conscience** – a director should act with intellectual honesty, in the best interest of the company, avoid conflicts of interest and remain independent in mind and action.

■

2. **Care** – a director should pay careful attention to the affairs of the company, a carefree or careless attitude is not acceptable.

3. **Competence** – a director should have the necessary knowledge and skills to exercise his / her duties and should continuously "upgrade" knowledge, e.g. keep abreast with IT development.

4. **Commitment** – a director should be diligent and prepared to put in the necessary time & effort.

5. **Courage** – a director should have the courage to take the risks associated with "directing & controlling" a company and should have the courage to act with integrity, even when there is pressure on him to act otherwise, or be unpopular.

■

Principle 1.2: **The board should ensure that the company is, and is seen to be, a responsible corporate citizen**

a) A very important aspect is "stakeholder interaction" and a significant part of this is the concept of the company reporting on its ***triple bottom line***, that is, the company's economic, social and environmental performance
   - ★ the **economic** aspect relates to the financial and non-financial information relevant to the company's business
   - ★ the **environmental** aspect includes the effect of the company's activities, products and services on the environment
   - ★ the **social** aspect embraces the values, ethics and relationships with the stakeholders of the company which the company promotes.

b) Being a good corporate citizen is far more than projecting an image & getting public relations right. It is about genuine commitment and leadership in the company, not a series of publicity stunts or a passing phase.

Principle 1.3: **The board should ensure that the company's ethics are managed effectively**

1. The board is responsible for creating & sustaining ethical corporate culture in the company. An ethical corporate culture requires that:
   - ❖ ethical practice for directors is a non-negotiable requirement;
   - ❖ sound moral values & ethics are propagated by the conduct of individuals (throughout the company);
   - ❖ business activity is directed by people with integrity, fairness, responsibility & vision;

- laws & regulations are obeyed; unfair practices, abuse of economic power (unfair treatment of suppliers) and collusion (e.g. price fixing) are avoided;
- "having to be ethical" cannot be used as an excuse for poor business performance;
- the directors duty is firstly to his company and shareholders, but the interests of ***all*** stakeholders must be considered.

2. Creating an ethical corporate culture requires that the company has a well-designed & properly implemented ethics management process consisting of the following four aspects:
   - **Compilation of an ethics, risks and opportunity profile**. An ethical risk would be doing business in a country / sector where bribery is rife. An ethical opportunity would be entering a business arrangement with a company with a well-known reputation for ethical conduct.
   - **Development of a Code of Ethics** which lays down ethical values, standards and specific guidelines for the company in its dealing with internal and external stakeholders.
   - **Integration of ethics** into the company's strategies and operations. This will include , ethical leadership, education and training for employees, communication of ethical requirements and advice on ethical issues which may arise, and the prevention and detection of misconduct e.g. by whistle blowing.
   - **Ethics performance reporting and disclosure**. The board should assess the company's ethical performance & disclose findings to internal and external stakeholders, in the integrated report.

Activity:
List four (4) aspects of a properly implemented ethics management process.

Feedback:
A well designed & properly implemented ethics management process consists of the following four aspects:

1. Compilation of an ethics, risk and opportunity profile.
2. Development of a Code of Ethics.
3. Integration of ethics into the company's strategies and operations.
4. Ethics performance reporting and disclosure.

BOARDS AND DIRECTORS

ELEMENT: Role and Function of the Board

1. The board should act as the focal point for and custodian of corporate governance
2. The board should appreciate that strategy, risk, performance and sustainability are inseparable
3. The board should provide effective leadership based on an ethical foundation
4. The board should ensure that the company is, and is seen to be, a responsible corporate citizen
5. The board should ensure that the company's ethics are managed effectively
6. The board should ensure the company has as effective and independent audit committee
7. The board should be responsible for the governance of risk
8. The board should be responsible for information technology (IT) governance
9. The board should ensure that the company complies with applicable laws and considers adherence to non-binding rules, codes & standards
10. The board should ensure that there is effective risk-based internal audit
11. The board should appreciate that stakeholders' perceptions affect the company's reputation

12. The board should ensure the integrity of the company's integrated report
13. The board should report on the effectiveness of the company's system of internal controls
14. The board and its directors should act in the best interests of the company
15. The board should consider business rescue proceedings or other turnaround mechanisms as soon as the company is financially distressed
16. The board should elect a chairman who is an independent non-executive director. The CEO of the company should not also fulfill the role of chairman of the board
17. The board should appoint the chief executive officer and establish a framework for the delegation of authority
18. The board should comprise a balance of power with a majority of non-executive directors. The majority of non-executive directors should be independent
19. Directors should be appointed through a formal process
20. The induction of and ongoing training & development of directors should be conducted through formal processes
21. The board should be assisted by a competent, suitably qualified & experienced company secretary
22. The evaluation of the board, its committees and the individual directors should be performed every year
23. The board should delegate certain functions to well-structured committees but without abdicating its own responsibilities
24. A governance framework should be agreed between the group and its subsidiary boards
25. Companies should remunerate directors and executives fairly and responsibly
26. Companies should disclose the remuneration of each individual director and certain senior executives
27. Shareholders should approve the company's remuneration policy

Principle 14: **The board and its directors should act in the best interests of the company**

a) A director:
   - ★ must not use his position to gain an advantage for himself, or knowingly cause harm to the company;
   - ★ must exercise his powers in good faith and for a proper purpose in the best interests of the company;
   - ★ must act with a degree of care, skill and diligence that is reasonably expected of a person

b) The personal interests of a director should not take precedence over those of the company. He needs to disclose any financial interest he may have at a meeting of the board.

Principle 16: **The board should elect a chairman who is an independent non-executive director. The CEO of the company should not also fulfill the role of chairman of the board**

a) The chairman should be:
   - ★ appointed on an annual basis;
   - ★ independent and not conflicted
   - ▪

b) The role of the chairman must be formalized, and his ability to add value, and his performance against what is expected of his role and function should be assessed annually.

▪

c) The chairman should focus on social, sustainability and transformation issues including employment equity, diversity management and social investment.
   - ▪

d) The board should have a succession plan in place for the position of chairman. Any former CEO of the company should not be eligible for appointment as chairman until three years have lapsed.

▪

e) The chairman should:

- ★ **not** be a member of the audit committee;
- ★ **not** chair the remuneration committee (may be a member);
- ★ **not** chair the risk committee (may be a member);
- ★ be a member of the nomination committee and may chair it

Principle 17: **The board should appoint the chief executive officer and establish a framework for the delegation of authority**

a) The CEO should:

- ★ play a critical and strategic role in the operation of the company;
- ★ ensure the long-term strategy and vision of the company is developed and implemented;
- ★ ensure a positive and ethical work climate is maintained;
- ★ foster a corporate culture that promotes sustainable ethical practices, encourages individual integrity and fulfills social responsibility objectives

b) The CEO should:

- ★ not be the chairman;
- ★ not be a member of the **remuneration**, **audit** or **nomination** committees, but should attend by invitation, recusing himself when matters of personal interest arise;
- ★ not take on the chairmanship of **other** companies (outside the group);
- ★ consider carefully the appropriateness of taking on non-executive directorships in other companies outside the group

Principle 18: **The board should comprise a balance of power with a majority of non-executive directors. The majority of non-executive directors should be independent**

Executive director:

- ★ a director who is involved in the management of the company and / or is a full-time salaried employee of the company;
- ★ may also be a non-executive director of another company

Non-executive director:

- ★ is not involved in the management of the company;
- ★ his role is to provide **independent** judgment and advice / opinion on issues facing the company;
- ★ has a duty of care, skill and diligence and should not take on more directorships than necessary

Independent non-executive director:

- ★ is not a representative of shareholder who has the ability to control or influence management;
- ★ does not have a direct or indirect interest in the company;
- ★ has not been employed by the company in any executive capacity for the preceding three (3) financial years;
- ★ is not a member of the immediate family of an individual who is, or has been during the previous three (3) financial years, employed by the company in an executive capacity;

★ is not a professional advisor to the company;
★ is free from any business or other relationship which could be seen to interfere materially with the individual's capacity to act independently;
★ does not receive remuneration contingent upon the performance of the company

The board should:

★ ensure that there is appropriate balance of power on the board i.e. it should not be dominated by an individual or grouping of individuals;
★ consist of individuals of integrity and courage;
★ have a suitable diversity of academic qualifications, technical expertise, industry knowledge, experience, nationality, age, race and gender to conduct the business of the board and make it effective;
★ have a CEO and a financial director;
★ have a structured program to rotate non-executive directors without losing necessary skills. At least one third of the non-executive directors should rotate every year.

Principle 19: **Directors should be appointed through a formal process**

a) The procedure for appointing directors to the board should be formal and transparent.
b) The board should thoroughly investigate the background of a proposed director before appointing or recommending an individual for appointment.
c) In the Companies Act 2008, careful attention must be paid to "Ineligibility and disqualification of persons to be a director".
d) It is also important to ensure that the proposed director has not been declared delinquent

Principle 20: **The induction of and ongoing training & development of directors should be conducted through formal processes**

The board should:

★ establish a formal induction program to familiarize the new director with the company's business & his responsibilities & fiduciary duties;
★ ensure new directors with limited experience are mentored;
★ ensure that formal processes (continuing professional development programmes) are in place to keep directors abreast of important matters such as changes in laws and regulations, accounting standards, etc., on an ongoing basis.

Principle 21: **The board should be assisted by a competent, suitably qualified & experienced company secretary**

a) The Companies Act 2008 makes it mandatory for a public company or state owned enterprise to appoint a company secretary.

▪

b) The board should appoint and remove the company secretary, but the company secretary should have a direct channel of communication to the chairman.

▪

c) The company secretary should:

★ have an arms-length relationship with the board;

- **not** be a director of the company;
- assist the nominations committee with the appointment of directors;
- assist with the director induction and training programmes;
- provide guidance to the board on the duties of the directors and good governance;
- ensure board and committee charters are kept up to date;
- prepare and circulate board papers;
- elicit responses, input, feedback, from board and board committee meetings;
- assist in drafting yearly work plans;
- ensure preparation and circulation of minutes of board and board committee meetings;
- assist with the evaluation of the board, committees and individual directors

Principle 23: **The board should delegate certain functions to well-structured committees but without abdicating its own responsibilities**

a) A committee may include persons who are not directors of the company, but that such persons

- Must not be ineligible to be or disqualified from being a director and may not vote on any matter decided by the committee.

b) King III recommends four standing committees, namely, **audit**, **risk**, **remuneration** and **nomination** committees.

- **Audit committee**: chairman should be an independent non-executive director

▪

- **Remuneration committee**: chairman should be an independent non-executive director
  - ▪ all members should be non-executive directors, majority of which should be independent

- **Nomination committee**: chairman should be the chairman of the board
  - ▪ All members should be non-executive directors, majority of which should be independent

- **Risk committee**: chairman should be a non-executive director

Members should include executive and non-executive directors, senior management and independent risk management experts where necessary

c) A director who is not a member of a specific committee may attend meetings of that committee, but may not participate in the proceedings without the consent of the chairman and will **not** have a vote.

Principle 25: **Companies should remunerate directors and executives fairly and responsibly**

a) The remuneration of directors is a very contentious issue, fuelled by frequent “scandals” reported in the press relating to huge bonuses paid to directors (even where the company has performed poorly), the granting of stock options to directors, etc. King III has addressed the issue comprehensively.

▪

b) Companies should have a remuneration committee which should recommend remuneration policies for all levels in the company but especially senior executives and non-executive directors.

▪

c) Non-executive director's fees should consist of a retainer and meeting attendance fee, and should be approved by the shareholders in advance. Non-executive directors should <u>not</u> receive incentive awards e.g. fees based on company performance.

-

d) Base pay and bonuses:
  - ★ remuneration should reflect the contribution of the executive measured against appropriate & defined criteria;
  - ★ annual bonuses should relate to performance against annual performance objectives;
  - ★ performance targets should be reviewed regularly and should be both financial and non-financial
  - ★ in measuring performance, multiple performance measures should be used to avoid manipulation of results or poor business decisions

e) Contracts and severance:
  - ★ employment contracts with executives should not commit companies to pay out large sums of money where the executive has been dismissed due to poor performance/failure;
  - ★ early termination of the contract (for other reasons) should not entitle executives to bonuses or share based payments in their severance pay

f) Share based and other long-term incentive schemes:
  - ★ shareholders should approve in advance, all long-term share based and other incentive schemes;
  - ★ incentive schemes should contribute to shareholder value & should be reviewed regularly to determine whether they fulfill this objective;
  - ★ participation in share incentive schemes should be restricted to genuine employees and executive directors and should be subject to appropriate limits for individual participation;
  - ★ the chairman and non-executive directors should not receive incentive rewards geared to share price or corporate performance;
  - ★ non-executive directors should not receive share options;
  - ★ share option awards should not be backdated and should not be exercisable within three years of the date of grant of later than ten years from the date of the grant

The table below is a summary of the composition of the board

	Board of directors
Chairman	Independent non-executive director CEO of the company should not also fulfill the role of chairman of the board
Membership	The board should comprise a balance of power, with a majority of non-executive directors. The majority of non-executive directors should be independent
Members	Minimum of two executive directors of which one should be the CEO and the other the director responsible for finance
Meetings	Meet at least four times a year

Board committees constitute an important element of the governance process. The table below sets out the composition of the different committees

	Audit Committee	Remuneration Committee	Nomination Committee	Risk Committee
Chairman	Independent non-executive director Chairman of the board should not be the chairman or member of the Audit committee	Independent non-executive director	Independent non-executive director	Independent non-executive director
Membership	All members should be independent non-executive directors	Majority should be non-executive directors of which majority should be independent	Majority should be non-executive directors of which majority should be independent The chairman of the board should be a member and may also be chairman	Executive and non-executive directors
Members	Minimum of three members	Not specified in King III	Not specified in King III	Minimum of three members
Meetings	Meet at least twice a year Should meet with internal & external auditors at least once a year without management being present	Not specified in King III	Not specified in King III	Meet at least twice a year

Activity:
List the responsibilities of the board regarding the induction of, ongoing training and development of directors.

Feedback:
The board should

- establish a formal induction programme to familiarize the new director with the company's business, his responsibilities & fiduciary duties;
- ensure new directors with limited experience are mentored;
- ensure that formal processes are in place to keep directors abreast of important matters such as changes in laws & regulations, accounting standards etc., on an ongoing basis

Activity:
What is an **independent non-executive director**? Describe the requirements which such a director must satisfy to be regarded as independent.

Feedback:
A non-executive director is a director who is independent of management and does not derive any remuneration for services rendered to the company (other than a director's fee).

Essentially it is a director who is not involved in the day to day running of the company, but in addition, is free of any of the following relationships with the company which could impair his independence:

- Is not a representative of a shareholder who has the ability to control or significantly influence management;
- Does not have a direct or indirect interest in the company which is material to the director or the company;
- Has not been employed by the company in any executive capacity for the preceding three financial years;
- Is not a member of the immediate family of any person described in the sentence above;
- Is not a professional advisor to the company;
- Is free from any business or other relationship which could be seen to interfere materially with the individuals capacity to act independently;
- Does not receive remuneration contingent upon the performance of the company

Activity:
The directors of School Projects (Pty) Limited are aware of the board's duty to present an integrated report which should include a remuneration report with certain disclosure. Uncertainty exists with regard to the disclosure that should be included in this remuneration report.

List the disclosure which should be included in the remuneration report as specified in the King III Report.

Feedback:
This report should be issued annually as part of the integrated report and should disclose/explain:

- The remuneration policies followed, the strategic objectives and the implementation of policies;
- The policy on base pay;
- Incentive schemes;
- Share incentive schemes;
- The salaries of the three most highly paid employees who are not directors;
- Material "ex-gratia" payments;
- The use of benchmarks;
- The remuneration of non-executive directors and committee fees

Activity:

Recently, whilst scanning through the annual report of Stadium Ltd, a company listed on the Johannesburg Stock Exchange (JSE), you came across the company's schedule of directors and committees.

These appeared as follows:

1. Board of Directors

Chief Executive Officer	-	Donald Winthrop
Managing Director – Administration	-	Charles Tree
Financial Director	-	Monty Mann
Operations Director	-	Christo Wells
Human Resources Director	-	Jerry German
Marketing Director	-	Koos Katswinkel
Non-executive Director	-	Caz Kallim
Independent non-executive Director	-	Mary Maswai

The company has not appointed a chairman. The most senior director who arrives at the directors' meeting acts as chairman.

2. Committees

2.1 Directors Appointment Committee	-	Donald Winthrop
	-	Charles Tree

This committee recommends to the shareholders who should be appointed as directors. If the two directors disagree, Donald Winthrop has the casting vote.

2.2 Remuneration Committee	-	Donald Winthrop
	-	Monty Mann
	-	Koos Katswinkel

2.3 Audit Committee	-	Monty Mann
	-	Christo Wells
	-	Mitchell Street (Internal Audit)
	-	External Audit
	-	Fred Carver (Financial manager)

All committees meet as and when required. The Board meets every six months.

3. Risk Committee

The Risk Committee was disbanded at the start of the year. The directors know the business and the risks involved.

Required

Comment on the information presented above in relation to the requirements of King III.

Feedback:

Stadium Ltd's adherence to King III appears to be lacking.

1. Board of Directors

1.1 The Board does not have a balance of executive and non-executive directors. At present, the Board consists of six executive directors, and two non-executive directors.

1.2 The majority of the non-executive directors are not independent.

1.3 The company has no chairman. King III recommends that a board should elect a chairman who is an independent, non-executive director.

1.4 The board of directors is the most important component of corporate governance and important decisions must be taken at board meetings. This requires that meetings be knowledgeably and efficiently run which, in turn, requires careful preparation for a meeting. At present, this does not happen and a meeting is simply run by the most senior director who arrives at the meeting. This also suggests that not all directors arrive for meetings.

1.5 The Board should meet at least four times a year. At present, the board meets every six months.

1.6 The Board appears not to reflect the diversity or demographics of South Africa (race and gender).

2. Committees

2.1 King III recommends that a company such as Stadium Ltd should have a Nominations Committee (it can be called the directors' appointment committee). This committee should be chaired by the chairman of the board, and all members should be non-executive directors, the majority of whom should be independent. At present Stadium Ltd doesn't have a chairman, neither Donald Winthrop nor Charles Tree are non-executive directors.

2.2 The recommendations for appointments as director should be made by the Board as a whole and not a select committee. A Nominations Committee will only assist in the process.

2.3 The Remuneration Committee should be chaired by an independent non-executive director and consist of a majority of non-executive directors of which the majority should be independent. At present, this committee has no independent, non-executive directors.

Donald Winthrop is again likely to carry the major influence. This committee will probably be seen to be looking after the interests of the directors, to the detriment of the company, by deciding on excessive remuneration packages for directors.

2.4 In terms of King III, the Audit Committee should be chaired by an independent, non-executive director, which Monty Mann is not, and it should be made up only of independent, non-executive members, which it is not.

2.5 Fred Carver, the financial manager, nor Mitchell Street, the internal audit manager, and the external auditor should not be committee members. These three groups should work closely with the committee at various times, but they should not be part of the committee.

2.6 All committees should schedule meetings properly and the audit committee should meet at least twice per year, not just on a random, “as and when” basis.

3. Risk Committee

3.1 Risk is an ever-present factor in any large company, and risks change. It is unrealistic for Stadium Ltd to think otherwise, and irresponsible to have disbanded the Risk Committee because the directors “know the business and the risks involved”.

3.2 Furthermore, it is an important part of integrated reporting that the company report on its sustainability to all stakeholders.

4. General

4.1 On balance, this company appears to be dominated by the chief executive officer (CEO), Donald Winthrop.

AUDIT COMMITTEES

ELEMENT: Existence of Audit Committees

1. The board should ensure that the company has an effective and independent audit committee.
2. Audit committee members should be suitably skilled & experienced independent non-executive directors.
3. The audit committee should be chaired by an independent non-executive director.
4. The audit committee should oversee integrated reporting.
5. The audit committee should ensure that a combined assurance model is applied to provide a co-ordinated approach to all assurance activities.
6. The audit committee should satisfy itself of the expertise, resources and experience of the finance function.
7. The audit committee should be responsible for overseeing of internal audit.
8. The audit committee should be an integral component of the risk management process
9. The audit committee is responsible for recommending the appointment of the external auditor and overseeing the external audit process.
10. The audit committee should report to the board and shareholders on how it has discharged its duties.

Principle 1: **The board should ensure that the company has an effective and independent audit committee**

a) The Companies Act 2008 makes it compulsory for a public company and a state owned company to have an audit committee.

▪

b) Meetings:
- ★ the audit committee should meet as often as is necessary but at least **twice a year**;
- ★ the audit committee should meet with internal & external audit (without management being present) at least **once a year**.

Principle 2: **Audit committee members should be suitably skilled & experienced independent non-executive directors**

a) All members should be independent non-executive directors & there should be at least three (3)members.

▪

b) The committee should collectively have sufficient financial knowledge, a good knowledge of financial risks.

c) At least one third of the members of the audit committee must have academic qualifications, or experience in economics, law, corporate governance, finance, accounting, commerce, industry, public affairs or human resource management.

Principle 3: **The audit committee should be chaired by an independent non-executive director**

The chairman of ***the board*** should ***not*** be the chairman of the ***audit committee***.

Principle 4: **The audit committee should oversee integrated reporting**

a) The board of a company may delegate its responsibility for reporting & internal control to the audit committee; the audit committee will make recommendations to the board which will, after evaluation, approve or reject them.

▪

b) The audit committee will be responsible for monitoring the integrity and completeness of the company's financial reporting. This will include:
- ★ evaluating judgments & reporting decisions e.g. changes in accounting policies, treatment & disclosure of significant or unusual transactions, compliance with IRFS and SA GAAP;
- ★ considering whether there are any conditions which may tempt management to "manipulate" the financial statements, e.g. bonuses for management linked to reported financial performance;
- ★ dealing with complaints & queries relating to previously published financial information;
- ★ acting as arbiter / referee between management and the external auditors when there is a disagreement on accounting matters;
- ★ confirming that other regulatory or enforcement requirements pertaining to the company's financial information is complied with e.g. JSE regulations for listed companies;
- ★ reviewing management's assessment of the company's going concern ability

c) The audit committees responsibility extends to the integrity & completeness of all price sensitive financial information including:
- ★ the integrated report & financial statements;

- ★ interim reports;
- ★ preliminary & provisional result announcements;
- ★ summarized financial information;
- ★ prospectuses

Principle 7: **The audit committee should be responsible for overseeing of internal audit**

The audit committee should:

- ★ be responsible for the appointment/dismissal, performance assessment of the CAE;
- ★ approve the audit plan;
- ★ ensure that internal audit is independent, and has the necessary resources, standing & authority to discharge its functions;
- ★ oversee co-operation between internal & external audit;
- ★ evaluate the effectiveness of internal audit by independent quality review;
- ★ report to the board on internal audit's assessment of the company's internal controls

Principle 8: **The audit committee should be an integral component of the risk management process**

The audit committee should have oversight of:

- ★ financial reporting risk;
- ★ internal financial control;
- ★ fraud risk (as it relates to financial reporting);
- ★ information technology risk (as it relates to financial reporting)

Financial reporting / internal financial controls

1. Although the board is responsible for the design, implementation and maintenance of a sound system of internal control, the audit committee should be responsible for overseeing risk management and controls.

▪

2. The audit committee must understand the environment in which the company operates and the challenges it faces, to be in a position to assess the appropriateness of the company's risk management programme.

▪

3. The audit committee should report annually to the board on the effectiveness of the company's internal financial controls. The report should include any financial control inadequacies which resulted in actual material financial loss.

▪

4. To be in a position to make this report, the audit committee should determine the nature and extent of a formal review of the design implementation & effectiveness of internal controls to be carried out (annually) by management or internal audit.

Fraud risks

1. The audit committee should consider matters which may result in material misstatements in the financial statements due to fraud.

▪

2. The audit committee should:
   - review the arrangements made to enable employees and outside whistle blowers to report concerns about improprieties in matters of financial reporting or compliance with laws & regulations which may affect financial reporting;
   - ensure that there is a suitable system in place for an independent and balanced investigation into matters reported by whistle blowers

Information technology risks

1. In most companies IT, internal control & risk are intertwined. In addition, IT has inherent risks which will need to be closely addressed.

▪

2. It is very likely that the audit committee will need expert IT advice to meet their responsibilities with regard to the management of the company's exposure to IT risk.

3. As a minimum, the audit committee should play an oversight role regarding:
   - IT risks and controls;
   - business continuity & data recovery;
   - data security and privacy

Principle 9: **The audit committee is responsible for recommending the appointment of the external auditor and overseeing the external audit process**

With regard to the external auditors, the audit committee should:

- ★ recommend the appointment, re-appointment and removal of the external auditors;
- ★ before making this recommendation (annually), assess the audit firm's & the designated auditor's qualifications, expertise & resources, effectiveness & independence;
- ★ approve the terms of the external auditor's engagement & remuneration;
- ★ oversee the planning & execution of the annual external audit;
- ★ define & implement a policy for the nature, extent & terms under which the external auditor may perform **non-audit** services;
- ★ review any accounting & auditing concerns arising from the internal or external audit;
- ★ develop a procedure for receiving, considering & resolving reportable irregularities;
- ★ at the end of the annual audit, review the quality & effectiveness of the audit process, by discussion with the external auditor, head of internal audit, finance directors, etc.; deviations from the original audit plan should be discussed

Principle 10: **The audit committee should report to the board and shareholders on how it has discharged its duties**

1. The report should provide, as a minimum:
   - ★ a summary of the role of the committee;
   - ★ whether the audit committee has adopted formal terms of reference, and whether it has complied with its terms of reference;
   - ★ names and qualifications of all members of the audit committee & the period for which they served;
   - ★ the number of audit committee meetings held & who attended;
   - ★ a description of how the audit committee carried out its functions;
   - ★ a statement as to whether the audit committee is satisfied with the independence of the external auditor;
   - ★ commentary on the financial statements, accounting practices & financial control of the company;
   - ★ information on other roles assigned to the audit committee by the board;
   - ★ recommend the integrated report for approval by the board

2. The report by the audit committee to the shareholders should be included in the integrated report.

Activity:
List the responsibilities of the Audit Committee regarding the appointment of external auditors

and overseeing the external audit process.

Feedback:

The Audit Committee should:

a. Recommend the appointment, re-appointment and removal of the external auditors;
b. Before making this recommendation (annually), assess the audit firm’s and the designated auditor’s qualifications, expertise and resources, effectiveness & independence;
c. Approve the terms of the external auditor’s engagement and remuneration;
d. Oversee the planning and execution of the annual external audit;
e. Define & implement a policy for the nature, extent and terms under which the external auditor may perform **non-audit** services;
f. Review any accounting and auditing concerns arising from the internal & external audit;
g. Develop a procedure for receiving, considering and resolving reportable irregularities;
h. At the end of the annual audit, review the quality and effectiveness of the audit process by discussion with the external auditor, head of the internal audit, finance directors, etc; and discuss deviations from the original audit plan

Activity:

The following is a summary of the composition of and certain functions of the Audit Committee of Mineco Ltd, a JSE-listed company in the mining sector of South Africa:

Audit Committee

Violet Mguni	-	Operations Director
William Smith	-	Government official (only attends Board meetings)
Bob Cilliers	-	Financial Director

The Audit Committee meets annually.

The Audit Committee evaluates the Board's performance. During a recent meeting of the Audit Committee, it was decided that Mineco Ltd would acquire shares in Africa Coal, a coal mining company listed on the JSE. A detailed analysis of the coal-mining sector supported this decision.

Required

Comment in terms of the requirements of King III on the information presented.

Feedback:

1. In terms of King III, the Audit Committee should comprise at least three members. Mineco Ltd has three members and therefore complies with King III.

▪

2. All members should be independent non-executive directors. Two members of the committee are not independent non-executive directors, as they are involved in the day-today running of the business.

3. The Audit Committee should meet as often as necessary, but at least twice a year.

▪

4. The board should be evaluated by the chairman or by an independent party, not by the Audit Committee.

5. As part of risk management, the Audit Committee cannot make decisions on the acquisition of shares in Africa Coal. This should be the responsibility of the Board (with the approval of the shareholders).

THE GOVERNANCE OF RISK

ELEMENT: The board's responsibility for risk governance

1. The board should be responsible for the governance of risk
2. The board should determine the levels of risk tolerance
3. The risk committee or audit committee should assist the board in carrying out its risk responsibilities

ELEMENT: Management's responsibility for risk management

4. The board should delegate to management the responsibility to design, implement & monitor the risk management plan

ELEMENT: Risk assessment

5. The board should ensure that risk assessments are performed on a continual basis
6. The board should ensure that frameworks & methodologies are implemented to increase the probability of anticipating unpredictable risks

ELEMENT: Risk response

7. The board should ensure that management considers & implements appropriate risk responses

ELEMENT: Risk monitoring

8. The board should ensure continual risk monitoring by management

ELEMENT: Risk assurance

9. The board should receive assurance regarding the effectiveness of the risk management process

ELEMENT: Risk disclosure

10. The board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders

Principle 1: **The board should be responsible for the governance of risk**

1. The board should have the responsibility to ensure that the company has implemented an effective ongoing process to identify risk, measure its potential outcome & activate what is necessary to manage the risks

Principle 3: **The risk committee or audit committee should assist the board in carrying out its risk responsibilities**

a) The board may appoint a risk committee to deal with risk management;

b) If a risk committee is appointed, it should:

- ★ be chaired by a non-executive director;
- ★ have a minimum of three (3) members (no limit);
- ★ consist of a mix of executive directors & non-executive directors, members of senior management & if necessary, independent risk management experts (who will not have a vote);
- ★ convene at least twice a year;
- ★ consist of members who have the qualifications, experience & skills to meet the responsibility of risk management, e.g. IT skills

c) The risk committee should:

- ★ specifically consider the risks which may affect the sustainability of the company and it may be appropriate to name the committee "the risk & sustainability committee";
- ★ review the risk management maturity of the company;
- ★ consider the risk management strategy & policies;
- ★ monitor the risk management process

Principle 4: **The board should delegate to management the responsibility to design, implement & monitor the risk management plan**

a) Management is accountable to the board for **designing**, **implementing** & **monitoring** the process of managing risk & integrating it into the day to day activities of the company.

b) Risks are very diverse, but it remains the responsibility of management, led by the chief executive officer, to manage those risks.

c) In larger companies, a chief risk officer (CRO) may be appointed to assist in managing risk.

Principle 5: **The board should ensure that risk assessments are performed on a continual basis**

1. In assessing risk, the board (risk committee) should take into account:

- ★ **stakeholder risks**: e.g. what risks will a proposed expansion of the company pose for the community in which the expanded business operation will take place? Increase in pollution, crime? Loss of recreational land?
- ▪
- ★ **reputational risks**: e.g. will the company suffer a loss to its reputation if it fails to support a particular cause or does not take appropriate action against a director convicted of fraud?
- ▪
- ★ **compliance risk**: in relation to legislation which significantly affects the company, e.g. what risks arise for the company if it does not implement the new Companies Act requirements adequately? Does an agreement with a competitor in the same business amount to price fixing?
- ▪
- ★ **ethics risk**: e.g. will the introduction of a bonus scheme for sales employees based on sales, increase the risk of unethical selling practices by sales personnel?
- ▪
- ★ **sustainability issues**: e.g. is the risk of loss of employees through HIV/AIDS on the increase?
- ▪
- ★ **corporate social investment, employee equity, BEE, skills development & retention**: e.g. is there a risk that valuable skills will be lost because of poor remuneration packages? Is there a risk that a new promotion strategy will fail to satisfy employee equity requirements?

▪

★ **human & financial capital**: e.g. is there a risk that a new venture will not generate sufficient cash flow to sustain itself? Will there be sufficient human skills available?

▪

2. Another framework for risk assessment may be to consider risk in the following categories:

★ **strategic risks**: e.g. the risks associated with adopting or changing company strategy, such as expansion of the manufacturing facility, entering a new market in a foreign country, acquiring another company

★ **operating risks**: e.g. risks relating to health and safety, and the environment for a chemical manufacturer

★ **financial risks**: e.g. the effect on cash flows should a company decide to move from a cash sales basis to a credit sales basis, or the risk associated with committing the company to long-term borrowing to finance an expansion

★ **information risks**: e.g. the risks associated with introducing electronic funds transfer for payment of creditors, or a retail company deciding to introduce on-line trading

★ **compliance risks**: e.g. the risk that a business decision may result in significant breaches of legislation, relating to pollution, the environment, taxation, price fixing, foreign exchange, fraud, etc.

Principle 7: **The board should ensure that management considers & implements appropriate risk responses**

Once risks have been identified, the board, risk committee and management, should consider the possible risk response options. The options include:

a) **avoid or terminate** the risk by not commencing or ceasing the activity which creates the exposure to the risk, e.g. if the company can no longer tolerate the risk of doing business in a foreign country, then close that business down

▪

b) **treat, reduce or mitigate** the risk, e.g. exposure to the risk of foreign exchange losses may be treated, reduced or mitigated by taking forward cover

c) **transfer** the risk to a third party, e.g. if the company consider that the proper maintenance of its computer system, database, etc., is at risk, it may decide to outsource this responsibility. Taking out insurance is a common method of transferring risk

▪

d) **accept** the risk, e.g. if a transport company's risk assessment reveals that a 100% increase in the cost of diesel to say R 15 a litre will seriously jeopardize its going concern ability, but that the risk of this occurring is low, the company may simply decide to accept the risk, rather than perhaps replacing its fleet of vehicles with more fuel efficient vehicles

▪

e) **exploit** the risk, e.g. where a retailer of expensive clothing anticipates loss of market share due to the economic downturn, it may decide to introduce a range of cheaper clothing to regain its market share

▪

f) **integrate** a number of options given above

Principle 10: **The board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders**

1. The board should report on how the company has dealt with risk management in a statement in the integrated report. The board should:
   - ★ include a statement that the board is responsible for the total process of risk management as well as forming an opinion on its effectiveness;
   - ★ disclose the system that is in place to evaluate the effectiveness of the process, e.g. independent reviews by internal audit;
   - ★ confirm that the board maintained a system to monitor changes in the company's risk profile;
   - ★ make a statement that key risks are being managed and that the board is not aware of any key risk, current, imminent or forecast, that may threaten the sustainability of the company;
   - ★ disclose any material losses (causes, quantity & effect) and steps which have been taken to prevent a recurrence.

Who is responsible for what? The table below sets out the responsibilities for the governance of risk.

WHAT	WHO
Governance of risk	The board
Design, implementing & monitoring the risk management plan	The board should delegate to management
Monitor risk management process	The board, Risk Committee, Audit Committee
Perform an objective assessment of the effectiveness of risk management	Internal audit

Activity:
Who is responsible for the governance of risk?

Feedback:
The board

THE GOVERNANCE OF INFORMATION TECHNOLOGY

1. The board should be responsible for IT governance
2. The board should ensure that IT is aligned with the performance and sustainability of the company
3. The board should delegate to management, the responsibility for the implementation of an IT governance framework
4. The board should monitor & evaluate significant IT investments and expenditures
5. IT should form an integral part of the company's risk management & the board should ensure that information assets are managed effectively

6. A risk committee and the audit committee should assist the board in carrying out its IT responsibilities

Principle 1: **The board should be responsible for IT governance**

IT governance is the responsibility of the board, either directly or through the risk committee or some other specifically formed “IT committee”

- board members should play an active role in IT strategy and governance
- the CEO should provide organization structures to support the implementation of the strategy
- the senior members of the IT division must be business orientated & must provide the link between IT and the business
- all executives should become involved in IT steering or similar committees such as an IT strategy committee
- IT matters should be a regular & significant part of the board’s agenda
- board members should challenge the IT department’s activities with the objective of uncovering issues, and problems, etc. are revealed
- the board should encourage management & IT to work together & should ensure that management understands the effect on the business of IT related risks
- the board should insist that IT performance be measured & reported to the board

Principle 2: **The board should ensure that IT is aligned with the performance and sustainability of the company**

IT governance should focus on:

- strategic alignment with the business & collaborative solutions, including the focus on sustainability. It is imperative that IT supports the objectives of the business & that IT and business managers collaborate in solving problems & developing both IT and the business itself
- value delivery, optimizing expenditure & proving the value of IT. The board should not approve IT projects before a thorough cost /benefit analysis has been done. Once a project is up and running, it should be regularly evaluated to determine whether the expected “return on investment” is being achieved
- risk management, safeguarding IT assets, disaster recovery & continuity of operations
- resource management, optimizing knowledge & IT infrastructure. This means that part of IT governance is ensuring that maximum (optimal) benefit is gained from the use of the IT resources which the company has as its disposal

Principle 3: **The board should delegate to management, the responsibility for the implementation of an IT governance framework**

a) Management should be primarily responsible for the implementation of the IT governance framework (structures, processes, mechanisms)

▪

b) An IT steering committee may be formed & a chief information officer (CIO) appointed by the CEO

▪

c) The CIO must have access to the board & should interact regularly with it on strategic IT matters

▪

Principle 4: **The board should monitor & evaluate significant IT investments and expenditures**

a) Whilst the investigation / feasibility studies relating to significant IT expenditures will be conducted by the IT steering committee, approval for the expenditure should come from the board

▪

b) The board should monitor the return on investment of major IT projects

▪

c) Intellectual property contained in the information system (e.g. unique software) should be protected

▪

d) Independent assurance on the governance of outsourced IT services should be regularly obtained

▪

Principle 5: **IT should form an integral part of the company's risk management & the board should ensure that information assets are managed effectively**

a) IT management must be able to demonstrate that:

- Effective disaster recovery plans are in place;
- The company is complying with relevant IT laws, rules, codes, etc.;
- Information is secure & protected from unauthorized access, contamination, destruction, etc.;
- Equipment is adequately safeguarded, e.g. from theft, damage, etc.

b) Information security has three components:

- **Confidentiality**: information should be accessible only to those authorized to have access
- **Integrity**: the accuracy & completeness of information & processing must be safeguarded
- **Availability**: authorized users have access to information when required

c) Sound IT security contributes for example, to:

- Building trust between the company & its business partners, customers & employees. Without this trust, new **business strategies** attempted are unlikely to succeed

▪

- **Sustaining normal business operations**, e.g. if a company's system "crashes" frequently & users cannot get information, the company will lose business

▪

- **Avoiding unnecessary** costs brought about by failure in IT security

▪

- **Meeting compliance requirements**. Companies are required to comply with the law in numerous ways. E.g.: a company must pay VAT. If the process of recording VAT is not secure & the database on which the VAT information is stored is not safeguarded, the amount of VAT indicated as payable may be inaccurate & incomplete or may not be available at all.

▪

Activity:

1. To whom should the board delegate the responsibility of implementing the information technology (IT) governance framework?
2. Who should assist the board in carrying out its information technology (IT) responsibilities?

Feedback:

1. Management is responsible for the implementation of the structures, processes & mechanisms for the IT goverenace framework. This could be achieved by appointing an IT steering committee. The CEO should also appoint a CIO who should be responsible for the management of IT.
2. The Risk Committee & the Audit Committee

COMPLIANCE WITH LAWS, RULES, CODES AND STANDARDS

1. The board should ensure that the company complies with applicable laws and considers adherence to non-binding rules, codes and standards
2. The board & each individual director should have a working understanding of the effect of the applicable laws, rules, codes & standards on the company & its business
3. Compliance risk should form an integral part of the risk management process
4. The board should delegate to management the implementation of an effective compliance framework & processes

Principle 1: **The board should ensure that the company complies with applicable laws and considers adherence to non-binding rules, codes and standards**

a) Where there are (legally) non-binding rules or standards which would enhance the company's corporate governance, the company should adhere to them. The company should disclose the applicable non-binding rules and standards to which it adheres on a voluntary basis in its reporting to stakeholders, e.g. there are numerous safety, environmental & industry standards which are recommended but are not "law".

▪

b) Exceptions, shortcomings and "loop holes" in the law should be handled ethically, & the company should not seek questionable ways of getting around the law; compliance should be an ethical imperative.

▪

c) The board should monitor the company's compliance with applicable laws, rules, etc. & the compliance should be a regular item on the agenda of the board.

▪

d) The integrated report should disclose details of how the board discharged its compliance responsibilities.

Principle 2: **The board & each individual director should have a working understanding of the effect of the applicable laws, rules, codes & standards on the company & its business**

1. The board has a duty to identify the laws, rules, etc., applicable to the company, and part of the induction & ongoing training of directors should be familiarization with applicable laws, rules, etc.

2. Not all directors need to have an in-depth knowledge of all the laws etc., applicable to the company. E.g. the production director is unlikely to have an in-depth knowledge of the Income Tax Act, but collectively the board must have in-depth knowledge & individual directors should have a sound knowledge of laws etc. applicable to their portfolios & at least an awareness of other laws, etc.

3. The company secretary has a duty to assist the board / directors in fulfilling their duties with regard to laws, regulations, etc.

Principle 3: **Compliance risk should form an integral part of the risk management process**

a) Compliance risk is the risk of damage arising from non-adherence to laws and regulations. Damage may be financial (e.g. losses from penalties, lost contracts), to the company's reputation (e.g. reports in the media about the company evading taxation), to stakeholder relationships (e.g. oil refinery breaches health regulations, and resultant pollution affects the local community) or sustainability e.g. bus company ignores roadworthy requirements placing its operations license in jeopardy.

▪

b) Like any category of risk, compliance risk should be identified, assessed and responded to through the company's risk management process.

▪

c) A compliance function may be established. It should:
- ➢ be independent
- ➢ provide assistance to the board & management in complying with laws, regulations, etc.
- ➢ be managed by a qualified & experienced person (compliance officer)
- ➢ report on its activities to the board / executive management
- ➢ be adequately resourced to fulfill its duties

Principle 4: **The board should delegate to management the implementation of an effective compliance framework & processes**

a) There should be a legal compliance policy, approved by the board & implemented by management.

▪

b) Compliance with laws, rules, codes & standards should be included in the **code of conduct** and management should inform & educate employees in respect of matters pertaining to compliance.

▪

c) A compliance officer may be appointed, and should be afforded access to the board to interact on compliance matters, e.g. the implementation of a new Act which affects the company and its employees.

▪

Activity:
State, with an explanation, whether the following statement is true or false:

The board and each individual director should have a working understanding of the effect of the applicable laws, rules, codes & standards on the company and its business.

Feedback:
True. The induction and ongoing training programmes of directors should incorporate an overview and any changes to applicable laws, rules, codes & standards.

INTERNAL AUDIT

1. The board should ensure that there is an effective risk based internal audit
2. Internal audit should follow a risk-based approach to its plan
3. Internal audit should provide a written assessment of the effectiveness of the company's system of internal control & risk management
4. The audit committee should be responsible for overseeing internal audit
5. Internal audit should be strategically positioned to achieve its objectives

Principle 1: **The board should ensure that there is an effective risk based internal audit**

a) Where a board decides not to establish an internal audit function, full reasons must be given in the integrated report. An explanation of how the company has obtained adequate assurance as to whether effective governance, risk management and internal controls have been maintained must also be given.

▪

b) Internal audit services may be provided by a department within the company or may be outsourced.

▪

c) Internal audit's key responsibility is to the board. It assists the board in discharging its governance responsibilities by:
   - ★ performing reviews of the company's governance process including ethics;
   - ★ performing an objective assessment of the adequacy & effectiveness of risk management &internal controls;
   - ★ systematically analyzing and evaluating business processes & associated controls;
   - ★ providing a source of information regarding fraud, corruption, unethical behavior and irregularities

▪

d) An internal audit charter should be formally defined, documented and approved by the board (audit committee)

▪

e) The internal audit function should adhere to the Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing and Code of Ethics.

▪

Principle 2: **Internal audit should follow a risk-based approach to its plan**

1. A compliance based approach to internal audit sets out to determine whether or not the company is complying sufficiently with internal controls & other rules and regulations. This is not regarded as sufficient by King III & the recommendation is that internal audit be risk based, i.e. the internal audit function gains a thorough understanding of the risks which the business faces as well as considering whether there are risks which have not been identified, and then conducts tests to determine that an appropriate risk management process is in place & being properly conducted.

2. A risk based audit approach to internal audit (as opposed to a compliance based approach) should be adopted. An audit plan should be developed & discussed with the audit committee. The plan should:

- ★ Address the full range of risks facing the company, e.g. strategic, operational, financial, ethics, fraud, IT, human & environmental
- ★ Identify areas of high priority, greatest threat to the company, risk frequency & potential change
- ★ Indicate how assurance will be provided on the risk management process & how the plan reflects the level of maturity of the risk management process
- ★ Have any changes to it, timeously, approved / ratified by the audit committee

Principle 4: **The audit committee should be responsible for overseeing internal audit**

a) Internal audit is the agent of the audit committee, the party which gets out & gathers the information which the audit committee requires to fulfill its responsibilities with regard to risk management.

▪

b) The internal audit plan should be agreed & approved by the audit committee.

▪

c) The audit committee should evaluate the performance of internal audit & ensure that it is subjected to an independent quality review.

▪

d) The audit committee should be responsible for the appointment, performance, assessment of the chief audit executive.

▪

e) The chief audit executive should report to the audit committee chairman.

▪

f) The audit committee should ensure that the internal audit department is appropriately resourced & funded.

▪

g) Internal audit should report at all audit committee meetings.

▪

Principle 5: **Internal audit should be strategically positioned to achieve its objectives**

1. The key elements in the success of the internal audit function are independence and objectivity.

2. It is important that the board ensures that internal audit is provided with the necessary “conditions” to attain & retain the status it requires to fulfill its role. For example:

- ★ The board and management should defend and promote the independence of internal audit;
- ★ Properly qualified & experienced staff with high ethical standards should be appointed to internal audit;
- ★ The directors and management should regard internal audit as an integral part of the assurance framework & an indispensable control mechanism in the risk management process;
- ★ Designating the head of internal audit as a senior member of the company, e.g. Chief Audit Executive (CAE);
- ★ Having the CAE report to the audit committee & administratively to the CEO;
- ★ Giving the CAE direct access to the chairman;
- ★ Supporting and being seen to support the recommendations of internal audit;
- ★ Ensuring that internal audit is sufficiently resourced and has an appropriate budget

3. If internal audit is to be granted the respect it deserves, its members must be competent, independent & objective as well as ethically sound.

4. Some of the tasks undertaken by internal auditors are complex and will require a thorough understanding of the latest tools & audit techniques, particularly in the information technology field.

▪

5. Internal auditors require appropriate business skills to enable them to understand the business & organizational dynamics of the company.

▪

6. The CAE will set the tone of the internal audit function & should have at least the following attributes:

★ strong leadership;
★ command respect for his competence & ethical standards;
★ be a strong communicator, facilitator, influencer, networker & innovator;
★ have a practical approach;
★ be able to think strategically & have strong business analysis skills

Activity:
List the responsibilities of the Audit Committee regarding the internal audit function.

Feedback:
The Audit Committee should:

★ agree to and approve the internal audit plan;
★ evaluate the performance of the internal audit function;
★ ensure that the internal audit function is subjected to an independent quality review;
★ ensure that the Chief Audit Executive (CAE) reports to the Audit Committee chairman;
★ appoint, assess the performance and dismiss the CAE if required;
★ ensure that the internal audit function is well resourced and has an appropriate budget allocated to the function;
★ ensure that the internal audit function reports at the Audit Committee meetings

Activity:
Stapleking Ltd is a large manufacturer & wholesaler selling a wide range of fasteners, such as staples, tacks & drawing pins. The company has a number of divisions, for example the commercial fasteners & domestic fasteners divisions. Controls are sound & include an internal audit department which is staffed by competent internal auditors. Internal audit activities are scheduled at the start of each financial year, but, during the year, numerous requests are received from within the company for “internal audit” to carry out various assignments. The following request have been received:

1. Lindsay Haffejee, the chief audit executive, has been asked by the human resources director to serve on a Selection Committee for the appointment of a new company secretary.

▪

2. The financial director has asked the internal audit department to design & implement a costing system for a new type of product which is to be manufactured.

▪

3. The information technology manager has asked internal audit to conduct a post implementation review of a recently introduced telesales ordering system.

▪

4. The warehouse manager has requested internal audit to perform an audit to determine whether the company is complying with all necessary safety regulations, for example fire protection & ventilation regulations.

▪

5. The financial director has requested internal audit to schedule an investigation into the payroll & personnel cycle to determine whether there are fictitious employees on the payroll.

▪

6. The production director has requested internal audit to conduct inventory cycle counts in the finished goods warehouse on an ongoing basis.

▪

7. The external auditors have requested internal audit to assist them with the verification of the existence of plant & equipment at an interim audit.

▪

8. The board of directors has requested internal audit to assist in identifying, evaluating and assessing significant organizational risks.

▪

9. The financial director has requested internal audit to perform an analysis of the monthly management accounts & to make a presentation to the board on a quarterly basis.

Required:

1. Explain how the board of directors can promote the status of the internal audit department

▪

2. Indicate, giving reasons, how Lindsay Haffejee, as the chief audit executive, should respond to the above requests

▪

Feedback:

1. **The board can promote the status of internal audit by**:

1.1 Appointing well-qualified staff in internal audit

▪

1.2 Designating the head of internal audit as a senior member of the company, for example chief audit executive

▪

1.3 Having internal audit report to the Audit Committee if there is one, or to the board itself (internal audit should report to the CEO in respect of administrative matters)

▪

1.4 Having internal audit (the head or representative) attend Audit Committee meetings

▪

1.5 Giving internal audit direct access to the chairman

▪

1.6 Supporting and being seen to support the recommendations of internal audit

▪

1.7 Developing a culture among the directors & management of viewing internal audit as an important & useful control mechanism which directly benefits them

▪

1.8 Ensuring that internal audit is properly staffed & resourced

▪

2. **Feedback on Lindsay Haffejee's requests**:

2.1 This request could be acceded to. The appointment of a company secretary is an important aspect from the point of view of corporate governance. In a sense the company secretary position is similar to that of internal audit, in that both are “control mechanisms”.

▪

2.2 This request should be refused. The design & installation of systems are an operational responsibility from which the internal audit department should be independent. Internal audit may review the proposed system & be part of the post-implementation review, but should not take responsibility for the system.

▪

2.3 This request should be acceded to. Part of internal audit’s basic function is to perform objective assessments of the adequacy & effectiveness of risk management & internal controls & post-implementation reviews are part of this.

▪

2.4 This assignment can be accepted. Although internal audit should follow a risk based approach to internal audit activities, compliance audits (evaluating whether the company is complying with relevant laws & regulations) are part of what internal auditors do. Ensuring compliance with laws & regulations is part of risk management.

▪

2.5 This assignment can be accepted. The board has direct responsibility for risk management, and for implementing & monitoring controls which, inter alia, safeguard the assets of the company (in this case, cash). Internal audit is part of the directors’ means of obtaining information relating to fraud & corruption.

▪

2.6 This request should be refused. Inventory control is an operational activity & is the responsibility of the inventory controller / production department. Internal audit could be used to review & evaluate cycle counts from time to time.

▪

2.7 This request can be acceded to. External & internal audit should cooperate in this kind of exercise which, in effect is an independent verification procedure.

▪

2.8 This request could be acceded to, but internal audit must not assume the functions, systems & processes of risk management in other words, become part of the operational internal controls. It is intended that internal audit assist & support the board in fulfilling its responsibilities, one of which is to identify risk. This request is in line with the risk based approach to internal audit.

▪

2.9 This assignment can probably be accepted. Internal audit is again fulfilling an independent evaluation role, as long as it does not become “responsible” for producing (part of) the management accounts, the assignment would be beneficial in assisting the Board to fulfill its duties. However, this does look a little like a financial/accounting section responsibility in the long run, but if it is the “independence” aspect which the financial director is after, it is probably acceptable.

NOTE: if there is an audit committee all requests for internal audit services would be discussed/accepted/rejected with & by the audit committee.

GOVERNING STAKEHOLDER RELATIONSHIPS

▪

1. The board should appreciate that stakeholders' perceptions affect a company's reputation
2. The company should proactively manage the relationship with its stakeholders
3. The board should strive to achieve the correct balance between its various stakeholder groupings, in the best interests of the company
4. Companies should ensure the equitable treatment of shareholders
5. Transparent & effective communication with stakeholders is important for building and maintaining their trust & confidence
6. The board should ensure disputes are resolved as effectively, efficiently and expediously as possible

Principle 2: **The company should proactively manage the relationship with its stakeholders**

1. The board should identify stakeholders relevant to the company's sustainability to ensure that they are accommodated in the reporting process.

▪

2. Managing stakeholder relations should be proactive. It is mainly about communication, both formal (AGM, meetings with regulators), but can also be through informal processes such as social functions, websites, media, etc.

▪

3. The major stakeholders and the underlying factors on which the relationships with these stakeholders should be built, are as follows:

   - **Suppliers**
     - It is in the interest of the company to have stable suppliers who supply products or services of the necessary quality at an acceptable price, when required.

     ▪

     - This is important for suppliers of strategic products or services e.g. a sugar milling company is entirely reliant on its transport supplier to deliver sugar cane to the mill if it has outsourced this function. Equally, the transport company will have invested heavily in capital expenditure & needs the contract with the sugar milling company to remain in business.

     ▪

     - A mutually beneficial relationship contributes to the sustainability of both companies.

   - **Creditors**
     - The company should be mindful of the fact that creditors, if not paid, have the power to have business rescue processes imposed on the company & in more serious situations, have the company liquidated.

     ▪

     - Creditors should be managed accordingly, paid on time at the correct amount. Payment terms should be fair to both parties.

▪

- Creditors are usually suppliers either of goods, services or finance and a mutually beneficial relationship should be developed. For example, a large supermarket chain should not push its payment terms for smaller suppliers to 120 days when they should be 60 days, just because they have the power to do so, knowing that the smaller supplier depends on the large supermarket chain.

▪

- **Employees**
  - Companies should engage their employees in improving the business ensuring that employees at all levels benefit from the improvement, e.g. incentive schemes, bonuses, etc.

  ▪

  - The company should also ensure that employees have the chance to develop their potential & capabilities by providing training, a healthy & safe working environment & the opportunity for employees to advance in the company.

▪

  - Proper leadership which includes strong communication with employees is essential. Failing to manage employees properly may result in low morale, poor productivity and work quality, strikes, “go-slows”, or even sabotage.

▪

- **Government**
  - A company should abide by the laws of the land & pay taxes due by it.

  ▪

  - All employees who deal with government should:
    - ➢ act in a manner which promotes mutual respect & co-operation;
    - ➢ not engage in an form of corruption

  ▪

  - Companies should not give “major gifts” to politicians or other government officials & should consider carefully whether it is appropriate to make financial contributions to political parties or similar groupings

- **External Auditors**
  - The company should not view the external audit function as an unnecessary cost or as a threat

  ▪

  - A properly conducted external audit will add immense value to a company. It adds significant credibility to the financial statements & is an integral independent element of the combined assurance model.

  ▪

  - External audit is appointed by & accountable to the shareholders.

  ▪

  - External audit works mainly with management & the audit committee, and company policy should promote co-operation between the parties, a free flow of information & appreciation of the independence requirements of external audit.

▪

- **Consumers / customers**
  - For customers to respect the company, the company:
    - ➢ should market responsibility e.g. not glorify products which can be harmful to health such as cigarettes, alcohol, certain food products;
    - ➢ should communicate production information e.g. content breakdown on foodstuffs, safety precautions for electrical products;

        - ➢ should not sell products which, e.g. are harmful to the environment, customers' health or which have been manufactured in labour "sweat shops" or under other adverse situations

- **Industry**
  - A company's sustainability is dependent on other entities within its sphere of operations. A company should therefore acknowledge its responsibility to its industry as a whole.

  ▪

  - To achieve this, a company should participate in or facilitate forums to address industry risks & opportunities.

  ▪

  - Companies should not engage in anti-competitive practices / price fixing.

- **Local communities**
  - Every company operates in a community to some degree or another. A community may be totally dependent on the company and in fact may have been created by the company, e.g. remote mine or forestry operation.

  ▪

  - Looking after its community, amounts to a company being a good corporate citizen, & should be geared to enhance the lives of local communities by health programmes, schooling, sporting opportunities, etc.

▪

- **Media**
  - It is important that a mutual relationship of trust be developed between the company & the media. If this is to be achieved, the company should be:
    - ➢ open to communication with the media;
    - ➢ accurate & truthful with the information it provides to the media;
    - ➢ professional in its approach e.g. not aggressive or condescending;
    - ➢ objective when assessing reporting by the media e.g. not overreacting with a journalist criticizes the company;

▪

- Likewise, the reporting journalist should:
  - ➢ be knowledgeable & experienced;
  - ➢ report accurately & fairly without sensationalism;
  - ➢ as with all forms of communication, the company is not expected to compromise its confidentiality standards or its competitive edge

- **Regulators**
  - The relationship between a company & its regulators is similar to that between a company & government. The company should comply with regulations, pay any fees due, deal with the regulators employees with professionalism & not engage in dubious practices to circumvent a regulation, e.g. attempt to bribe an official who is carrying out a regulatory health inspection.

- **Potential investors**
  - Potential investors, i.e. those who may be seeking to invest as opposed to existing shareholders, will expect high standards of corporate governance, board integrity & confidence in the sustainability of the business of the company.

  ▪

  - To enable potential investors to evaluate these aspects, clear and transparent disclosure should be available to them, e.g. on a website, contained in media releases, etc. Frequently large companies will meet with financial journalists & potential institutional investors (e.g. pension funds) to communicate this information.

▪

Principle 3: **The board should strive to achieve the correct balance between its various stakeholder groupings, in the best interests of the company**

1. It is often perceived that the most important stakeholders in the company are the shareholders and that the board's major responsibility is to this body, e.g. profits must be made, share prices maintained, etc.

▪

2. However, the interests of different stakeholders may well clash & it is in these situations that the board should attempt to satisfy the needs of all shareholders. This provides a better chance of sustaining the company. For example, a fertilizer company may want to expand its operations. It has a choice of two sites. Transport & construction costs on site A will be much cheaper & the company will earn a far greater return on investment if it expands to site A. However, expansion on site A will also negatively affect the local fruit farming community. Site B will be expensive for the company to develop and return on investment will be lower, but there will be no negative affect on local business, and job opportunities will be created for the local community. Does the board go for site A or site B?

Principle 4: **Companies should ensure the equitable treatment of shareholders**

1. Not all shareholders are equal. There are different classes of share with different rights. There are majority shareholders & minority shareholders, and controlling shareholders & non-controlling shareholders.

▪

2. Despite this, shareholders must be treated fairly. For example, minority shareholders should be protected against the abusive actions of majority or controlling shareholders.

▪

3. The Companies Act 2008, Chapter 7 provides remedies for aggrieved parties (including shareholders), but wherever possible the board should set up processes which allow for constructive engagement to minimize the costs & time taken up by the more formal remedies.

Principle 5: **Transparent & effective communication with stakeholders is important for building and maintaining their trust & confidence**

1. If stakeholders do not receive information which is sufficient, relevant, accurate, honest & timeous, the communication of the information is unlikely to contribute to meaningful stakeholder involvement in the corporate governance process.

▪

2. Information should be provided on both the negative & positive aspects of the company's performance, & attention should be paid to the wording of negative situations. The negatives should not be hidden behind complex / technical language designed to confuse stakeholders.

▪

3. Whilst transparency is important, what is disclosed must be considered in the light of:
   - ★ legal requirements including those applicable to access of information and
   - ★ the maintenance of the company's competitive advantage

▪

4. The board should also consider the suitability of the method used to communicate, e.g. an information website may be a cheap and effective method but stakeholders, such as a local labour community, may not have easy access to computers.

Principle 6: **The board should ensure disputes are resolved as effectively, efficiently and expediously as possible**

1. In terms of their duty of care, directors are required to resolve disputes effectively, efficiently and as quickly as possible.

▪

2. It is the board's duty to set up mechanisms / processes to resolve disputes, e.g. where a dispute arises with an employee, there must be a laid down procedure for that employee & the company to follow. Where there is a dispute (e.g. unlawful strike) with a labour union, there is an established legal procedure which must be followed; the company must have processes in place to adhere to the legal procedure.

▪

3. Disputes can be internal (e.g. with an employee or shareholder) or external (e.g. with a supplier, customer, local community), and are simply a part of "doing business". Obviously disputes can be taken to court but this is generally costly and time consuming.

▪

4. Alternative dispute resolution (ADR) is now a widely accepted practice which involves the parties to the dispute taking the matter to arbitration, adjudication or mediation. This essentially amounts to a party independent of the disputing parties, hearing both sides of the dispute and "presenting a finding or solution".

▪

5. The company should select a dispute resolution method that best serves the interests of the company. For example, going to court, arbitration or adjudication results in a judgment, whereas mediation or conciliation allows the dispute parties and an impartial and neutral third party to work together to negotiate a resolution to their dispute. (A settlement agreement rather than a handed down judgment).

▪

6. In deciding on which dispute resolution method to follow, the board should consider at least the following factors:

★ **time available to resolve the dispute** – court proceedings can continue for years with postponements, appeals, etc. ADR can be concluded much quicker. It is usually in the interests of the disputing parties to resolve the matter promptly.

▪

★ **principle and precedent** – where the company wants a binding decision on an important matter of principle, which will result in a precedent for any future disputes, a court action is likely to be more suitable.

▪

★ **business relationships** – ADR, especially mediation/conciliation is normally far more "friendly" than court proceedings. It is important to maintain good business relationships (sustainability) and mediation / conciliation is more likely to contribute to the continuation of good business relationships.

▪

★ **expert recommendations** – where the parties do not wish to go to court, but do not have the necessary expertise to devise a solution, an expert may be required to facilitate a solution (this is conciliation).

▪

★ **confidentiality** – where confidentiality for the dispute parties is very important, ADR may be more suitable as dispute resolution proceedings may be conducted in confidence.

▪

★ **Rights and interests** – court proceedings, arbitration and adjudication results in the decision maker imposing a resolution on the parties based on the principles and rights applicable to the dispute. Mediation and conciliation allow the parties a level of flexibility in fashioning a mutually beneficial solution.

▪

★ **empowerment of participants** – if mediation or conciliation is to be promptly & successfully concluded, the personnel involved must be given the necessary powers to act.

▪

7. The success of ADR is largely dependent on the willingness of the parties to resolve the dispute. Obviously presentation skills, a thorough knowledge of the subject matter of the dispute & a professional approach are pre-requisites. Those who fall short of the “will and capacity” to resolve the dispute, should be excluded. Thus the board should select the appropriate individuals to represent the company in ADR.

Activity:

State, with an explanation, whether the following statement is true or false:

The stakeholders of the company consist of only the shareholders and the employees.

Feedback:

The statement is false. Stakeholders are any group which can affect, or be affected by the company, such as shareholders, employees, creditors, lenders, suppliers, customers, regulators, the media, analysts, the community in which the company may operate, etc.

INTEGRATED REPORTING AND DISCLOSURE

1. The board should ensure the integrity of the company’s integrated report.
2. Sustainability reporting & disclosure should be integrated with the company’s financial reporting.
3. Sustainability reporting & disclosure should be independently assured.

Principle 1: **The board should ensure the integrity of the company’s integrated report**

a) For the company to be transparent & accountable to all of its stakeholders, effective communication is essential. This means that reporting by the company should be:
   - ➢proactive
   - ➢relevant and transparent
   - ➢cover all material matters affecting the company
   - ➢integrated across all areas of performance and

➢include reporting on **economic**, **social** & **environmental** issues (triple bottom line)

b) There should be controls in place e.g. verification & review of data, to ensure the integrity of the integrated report.

▪

c) The audit committee should evaluate sustainability disclosures.

▪

d) Transparency in reporting sustainability information is critical if the trust and confidence of the stakeholders in the company is to be maintained.

▪

e) Transparency requires that both the positive & negative be reported on, and where negative matters are reported, the company's plans to reduce the effect of this should be disclosed.

▪

f) Sustainability reporting should address the needs & expectations of both internal stakeholders (e.g. employees) and external stakeholders (e.g. the local community)

▪

g) Although transparency is a key requirement for sustainability reporting, confidential information should not be disclosed. Obviously, non-stakeholders will have access to what is reported and should not be provided with an easy opportunity of acting in a manner which may harm the company.

▪

h) The integrated report should be prepared every year.

▪

Principle 2: **Sustainability reporting & disclosure should be integrated with the company's financial reporting**

a) If a company decides to report on its HIV/AIDS prevention activities, the reporting system should be able to provide the information necessary to make the report meaningful for stakeholders.

▪

b) The integrated report should contain commentary on the financial results, going concern, and how profits have been made (or losses suffered).

▪

c) Reporting to stakeholders is not just a matter of compiling the annual report and making it available to stakeholders.

▪

d) Each company will have different stakeholders & stakeholders will have different information needs, so each company should decide on the frequency and method of reporting to its stakeholders.

▪

e) The method of reporting may include meetings, e.g. feedback sessions on pollution to the community in which a company has its manufacturing operations, written reports, e.g. the annual report, or posting information on the company's website. There a number of standards to assist companies in deciding on what is most suitable for their circumstances.

▪

▪

Principle 3: **Sustainability reporting & disclosure should be independently assured**

a) General oversight for sustainability reporting should be delegated to the audit committee.

▪

b) The audit committee should review the integrated report to ensure that information is reliable, relevant, understandable & complete.

▪

c) The audit committee may seek the provision of independent assurance.

-

Activity:

Briefly explain the term “triple bottom line” reporting.

Feedback:

It refers to the practice of a company reporting not only on a single bottom line, i.e. profits, but rather on its economic, social and environmental activities.

Activity:

Treelines Ltd is a large forestry company which grows and harvests trees & transports them to its mills where the timber is pulped (an operation which uses a great deal of water & produces unusable waste) for the manufacture of pulp based products. Demand for pulp based products is declining worldwide, but demand for other timber products is stable.

The company’s forests are spread over numerous regions of the country, and the majority are in remote areas. A key element of the location of forests for both replanting (once trees have been harvested) and new forests is the level of local rainfall as forests are not irrigated.

Treelines Ltd employs a reasonably large workforce at its forest locations – a workforce ranging from unskilled to skilled logging machine operators all of whom are vital to the operation. It also has a large administration, financial, marketing & support staff of mixed gender and race at its head office.

The Board of Treelines Ltd adopts sound corporate governance in how it conducts its business & in how it reports to its stakeholders. Integrated sustainability reporting & disclosure are regarded as an important part of keeping stakeholders informed, and of building & maintaining relationships & promoting respect between the company and the stakeholders.

Required:

1. Discuss how frequently a company like Treelines Ltd should report to its stakeholders on sustainability & other issues.
2. Identify the main stakeholders, other than shareholders, with whom Treelines Ltd should be “building & maintaining relationships and promoting respect”, and indicate briefly, in respect of each, why you consider them to be stakeholders.
3. Identify & briefly discuss, based on the information about Treelines Ltd given in the question, the sustainability issues which the company should report on in its integrated report.

Feedback:

1. King III states that effective reporting should take place at least once a year, but there is no fixed number of times it should take place. The objective is to keep all stakeholders informed to the extent that satisfies each stakeholder group’s needs.

-

2. Treelines Ltd’s main stakeholders are:

    -

-

2.1 **Suppliers** of goods and services without whom the company cannot operate effectively.

-

2.2 **Creditors** arising from the supply of goods, services & finance, e.g. loan providers. These parties are owed money & therefore have a direct stake in the company.

▪

2.3 **Employees** at all levels and in all activities, skilled, unskilled & administrative.

▪

2.4 **Government** and important parties responsible for relevant legislation, e.g. governing the granting of forestry licences.

▪

2.5 **External auditors**, who require cooperation and respect to fulfill their legislated function.

▪

2.6 **Customers** who may range from individual to large corporations to government and who are the lifeblood of the company.

▪

2.7 **Industry at large** – Treelines Ltd does not operate within a vacuum. It is part of the greater economic community & of the forestry / milling / pulp / paper industry specifically. Cooperation & participation are key to the sustainability of the industry as a whole.

▪

2.8 **Local communities** – companies are part of a wider society & as in the case of Treelines Ltd of numerous local communities. The company depends on these communities & vice versa.

▪

2.9 **The media** – financial, industrial and human interest journalists write about companies & can enhance or damage a company's reputation & its image as a good corporate citizen. They have a "stake" in the company & the company needs to manage relationships accordingly.

▪

2.10 **Regulators** – Treelines Ltd will probably be regulated by a number of bodies that require compliance with rules, regulations or a code, e.g. the Forest Stewardship Council regulations and code. A sound working relationship between the company and regulator must be promoted.

▪

3. Sustainability issues which should be reported on:

3.1 The declining demand for pulp based products & its anticipated effect on Treelines Ltd's business:

★ Whether mills will be temporarily closed or shut down permanently
★ Whether retrenchments are likely
★ Whether replanting or new forests are intended

3.2 The board's response to the decline in pulp based products, including any plans to diversify into other timber products.

▪

3.3 How environmental issues are being addressed:

★ Reduction of water usage at the mills
★ Reduction of CO_2 and other harmful emissions
★ Reduction of unusable waste

3.4 Incidents of fire in plantations & the prevention thereof.

▪

3.5 Monitoring of weather patterns and trends in forestry areas with regard to replanting & new forests.

▪

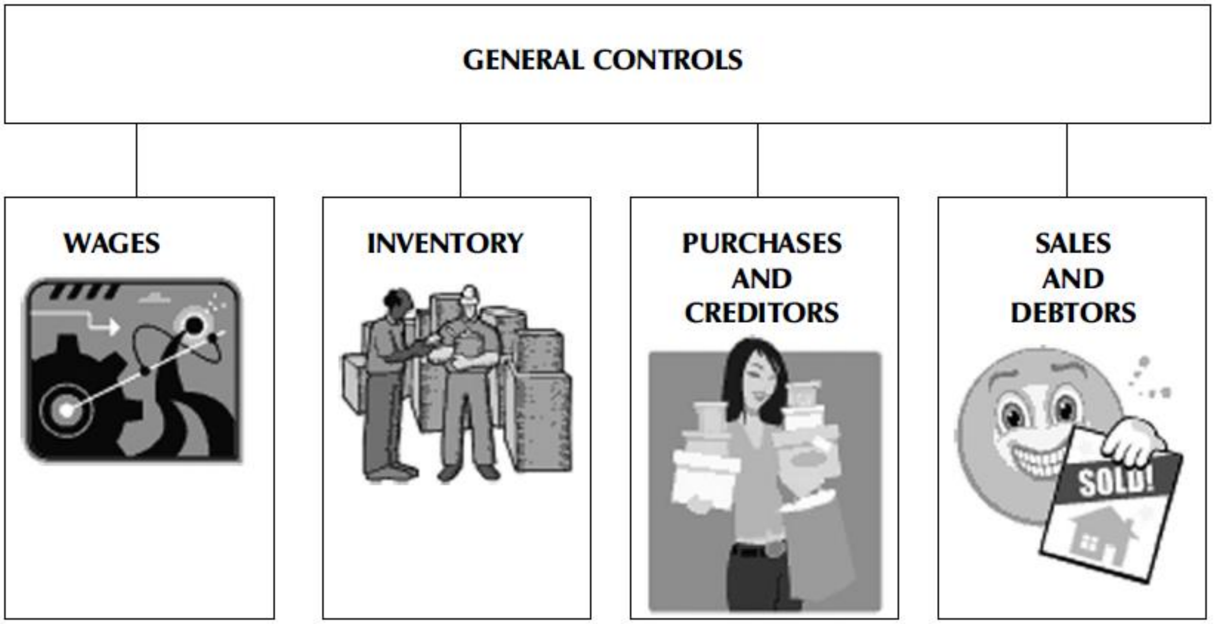
3.6 How employees throughout the company have been enhanced:

- ★ Ongoing training of all levels
- ★ Development of gender and race at management level

3.7 Relations with remote local communities;

- ★ Training of locals in essential forestry skills;
- ★ Provision of decent living conditions, transport and education
- ★ Health programmes, e.g. provision of HIV / AIDS drugs & counseling
- ★ Prevention of injury to forest workers

Control environment



1. **Communication and enforcement of integrity and ethical values**
   - In terms of King III, ethical IT governance must be cultivated & promoted & should align with the ethical culture of the organization.
   - A strong ethical culture is important in an IT department, particularly as IT personnel will have access to confidential & sensitive information, and may also have the opportunity to cause disruption to operations & destruction & unauthorized alteration of data.
   - IT management should communicate a code of ethical behavior, comply with it themselves, and take strong remedial action which may include dismissal where integrity & ethical behavior have been lacking.

2. **Commitment to competence**
   - The demands of the IT department with regards to skill and knowledge can be considerable.
   - IT management should be committed to matching these attributes to an individual's job description. Again the consequences of an individual not being able to do his job could be immense. Performance reviews & regular discussions with employees assist in achieving this.

3. **Participation by those charged with governance**
   - IT governance is the overall responsibility of the board and it should provide the required leadership & direction to ensure that IT achieves, sustains and enhances the company's strategic objectives.
   - There should be defined mechanisms for the IT department to communicate with the board and report regularly to it.
   - The board should appoint an IT steering committee to assist with the governance of IT. A steering committee is a group of people knowledgeable about computers, to whom major issues are referred, e.g. policies, future strategy, IT risk, acquisitions of hardware & software
   - The IT department should not be seen as a "separate entity" only answerable to itself.

4. **IT management's philosophy and operating style**

➢ IT's actions set the tone of the department and as they lead, so will the employees follow. Their management philosophy and management style must demonstrate, communicate and enforce sound control.

➢ Very often IT personnel are seen as technical specialist who are more interested in IT and the excitement of its capabilities, than they are in the financial side. This can lead to a level of disharmony within management.

5. **Organisational structure and assignment of authority and responsibility**

5.1 The organizational structure should achieve two major objectives:

★ It should establish **clear reporting lines / levels of authority**; and

★ It should lay the foundation for **segregation of duties** so that no staff perform incompatible functions

5.2 The organizational structure should address segregation of IT and **user** departments & segregation of **duties within the IT department**.

▪

5.3 In terms of King III the chief executive officer should appoint a chief information officer (CIO) who is suitably qualified and experienced. This individual should interact on a regular basis with:

★ the board;

★ steering committee and audit committee

★ executive management

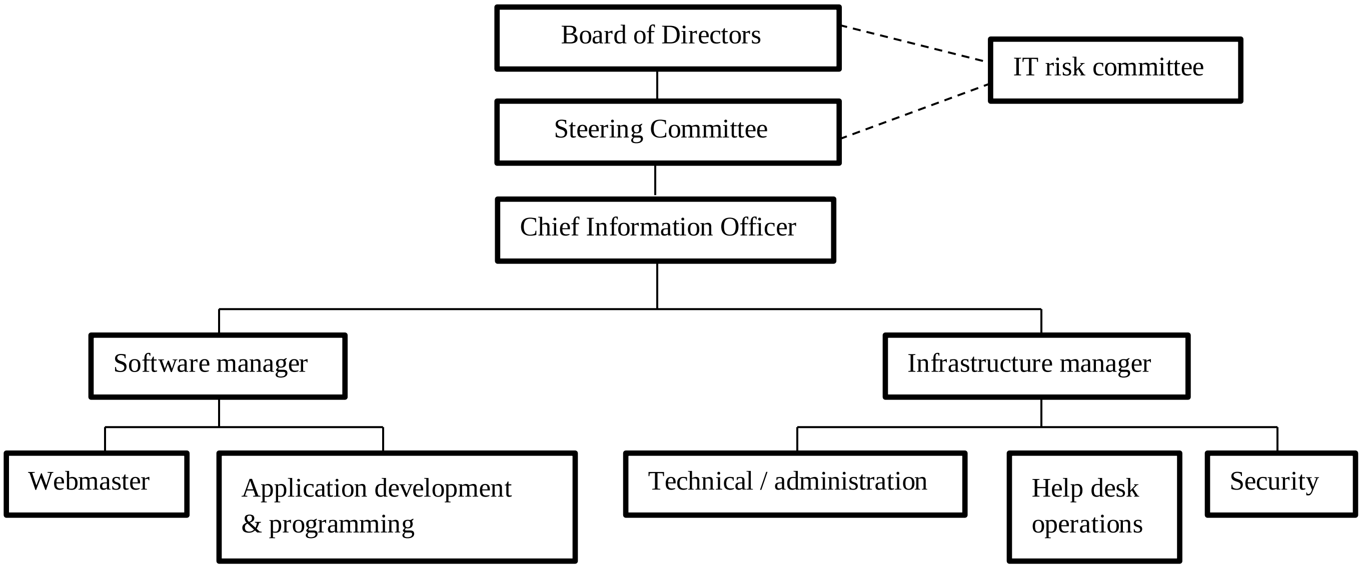
5.4 Overall the functions of supervision, execution and review within the department should be segregated as far as possible.

▪

5.5 Job descriptions, levels of authority and responsibilities assigned to IT personnel should be documented.

▪

Sound Organizational Structure for an Information Technology Department



- **Application development and programming**
  - **Business / systems analysts** – are responsible for liaising with users to understand their needs & documenting functional specifications for new applications & programme enhancements.
  - **Programmers** – write the programme code based on the specifications supplied by the business analysts, document the technical specification & debug programmes.
  - **Webmaster** – a webmaster should be appointed. Responsibilities will be to:
    - design, develop and maintain the company's website;
    - regulate and manage the access rights of the users of the site;
    - set up and maintain website navigation;
    - deal with complaints and other feedback about the site
  - **Technical / Administration**

    (a) **Database administrators** – have the specialized skills to develop, maintain and manage the database (the store of information);

    (b) **Operating system administrators** – have the specialised skills to implement, maintain & manage the operating system & hardware;

    (c) **Network administrators** – have the specialised skills to implement, maintain & manage the company's LAN/WAN, etc
  - **HelpDesk / Operations**
  - Helpdesk operators receive calls from users & log their problems / requests on the HelpDesk System as well as performing routine operational duties e.g. checking backups have been completed successfully & managing rotation of backup tapes.
  - **Security personnel** lay down control procedures for access to all computer facilities, monitor security violations (e.g. logs) and follow these up, issue passwords.
  - **The IT department should be entirely separate from user departments**
    - No transactions should be authorized or executed by any member of the IT department, e.g. placing a purchase order or authorizing a wage rate increase
    - No member of the IT staff should have access to, or custody of, the physical assets of the company, e.g. inventory, or uncontrolled access to the non-physical assets, e.g. the debtors masterfile
    - IT staff should only be responsible for correcting errors which arise from operating or processing problems; unless in response to authorized requests from user departments for assistance with corrections

6. Human resource policies and practices

The characteristics of honesty, competence and trustworthiness are paramount in a computerized environment & management should institute the following policies and practices:

- ★ Proper recruiting policies which include careful checks on an applicant's background & competence.
- ★ Immediate exclusion from computer facilities if an employee is dismissed (password and user privileges should be cancelled).
- ★ Compulsory leave – employees who are involved in unauthorised activity will often be uncovered when they are not present to cover their tracks.

- Training and development to keep staff up to date & able to fulfill their functions efficiently & effectively.
- Written formalization of human resource policies to provide employees with terms of reference or guidelines.
- Rotation of duties – moving employees between functions, is a useful practice as it helps avoid undue reliance on any individuals by ensuring that each employee has a backup. It may also relieve boredom as well as encourage employees to develop new expertise & skills. Rotation of duties should not be implemented to the extent that segregation of duties is compromised, e.g. the computer operator should not be trained as an application programmer & then be placed temporarily in the programming section.
- Strict policies pertaining to the private use of computer facilities by IT personnel (and other employees) should be in place, e.g. internet use and running private jobs.

The following example indicates that an effective control environment is present:

- Management takes computer information processing seriously.
- Aspects pertaining to computer information processing are effectively managed and any risks are immediately dealt with.

It is clear that the functions of the user department should be completely separated from the functions of the information technology department. This is illustrated by the following examples:

- The information technology department should not initiate or authorise transactions;
- The information technology department may not authorise amendments to a masterfile;
- The user department must check all amendments to a masterfile;
- Personnel in the IT department should not be permitted to correct errors made by the user department.

Further, certain functions in the electronic data processing section should also be segregated to promote internal control.

Activity:

Indicate, in each of the following cases, whether or not the internal controls were undermined.

1. Transactions rejected during data processing are corrected and re-entered by the CIS department.
2. Payroll operators have to sign when they take over the payroll masterfile from the programmer. The programmer should in turn ensure that the files are in safekeeping.
3. All members of staff are fully trained in the operation of all programs and are able to operate all programs.

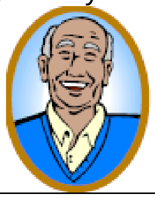
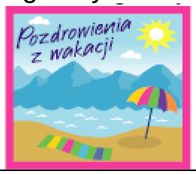
Feedback:

1. The principles are not being undermined. The CIS department should correct its own errors.
2. The principles are being undermined. Masterfiles should be kept under the supervision of an independent person.
3. The principles are being undermined. All members of staff may be fully trained, but particular tasks and responsibilities must be reserved for specific people. Access to functions could be restricted by means of passwords.

Management should introduce controls to ensure the following:

- That the staff appointed are honest and competent;
- That the staff are satisfied;
- That the work produced by staff is of a high standard

To achieve the above aims, it is necessary to develop a policy that includes the following aspects of personnel practice:

Personnel practices	Explanation of the principle with reference to an example
Proper recruiting policies 	Background checks should be carried out: referees on a CV must be contacted and proof of qualifications requested before a person is appointed.
Immediate exclusion from computer facilities if an employee is dismissed or leaves the service of the company for any other reason. 	Mr X reaches retiring age and leaves the service of the company. On the last day of his service Computer Services must cancel Mr X's access to all systems and programs.
Compulsory vacation leave/staff must take vacation leave regularly. 	Mrs Y has taken no leave in the last year. She is contravening the management policy that requires employees to use their leave allocation for a particular year in that year. Management should compel Mrs Y to take her annual leave in the following month.
Training and development 	Management must identify courses and seminars on a regular basis and request certain members of staff to attend the courses since this will make them more efficient in carrying out their duties and expand their skills.
Formalisation of personnel practices 	All the personnel practices must be formalised in a written procedural manual that codifies the policies regulating personnel practices. This manual must be freely available and must be regularly revised and updated.
Rotation of duties 	Staff must be rotated so that cross-training can take place. If Mr R goes on leave Mr V is available to do his work successfully. This practice prevents boredom, because if someone stays in the same job for years errors can easily creep in.
Strict policies pertaining to the private use of computer facilities	Certain websites should be blocked during office hours, for example, facebook.

Systems Development and Implementation Controls

New systems are continually being developed, but often without adequate systems development procedures and documentation. As a result a system might generate inaccurate or incomplete records that could increase the possibility of fraud.

Why do you think systems development and implementation controls are important?

Systems change because the business world changes and the need for quicker, different, additional and better quality information increase. Business related systems are said to have a "life cycle", they start, develop, mature & decline. Changes in the company's information system may arise because of changes in the company's business activities, growth, a need to maintain a competitive advantage or just to improve it all round performance by having better information. Unless the designing of a system is carefully controlled, the following might occur:

★ costs of development may get out of control;
★ the system design may not suit user requirements properly;
★ programs within the system may contain errors and bugs;
★ important financial reporting requirements are not incorporated into the system or are incorrectly understood by the business analyst / programmer;
★ the new system may not incorporate enough controls to ensure the integrity of its programs & data, e.g. the design of access privileges may give employees write access to programmes they should not have any access to;
★ an excellently designed system may be rendered virtually useless because no-one knows how to use it;
★ the information transferred from the old system to the new may be erroneous, invalid or incomplete

If proper systems development and implementation controls are put in place, the risks mentioned above can be avoided.

1. For in-house development and implementation of systems

1.1 **Standards**

➢ All systems development should be carried out in accordance with pre-defined standards which have been set for each of the phases described below, e.g. components of the ISO 9000 series of standards.
➢ Compliance with these standards should be strictly monitored and any deviations strictly followed up by management.

1.2 **Project approval**

➢ Projects for systems development may arise out of user requests or as a result of strategic planning.
➢ A feasibility study should be carried out:
  - a system specification for an in-house development proposal;
  - a proposal which involves the purchase of off-the-shelf software;
  - rejection of the project

▪ The feasibility study should include a cost / benefit analysis which lists and puts a money value to:

- all requirements for the project such as personnel, hardware, software & running costs;
- all benefits arising e.g. increased revenue, reduced costs, improved controls

- The steering committee should give its approval prior to commencement of the project

1.3 Project management

- A project team should be formed by the steering committee to manage the project & should include IT & appropriate user personnel, including accounting and internal audit personnel.
- The development project should be planned in stages, each stage detailing the specific tasks which must be completed.
- Responsibility for each task must be allocated to appropriate staff members.
- Deadlines should be set for completion of each stage and each task.
- Progress should be monitored at regular intervals to identify any problems which may affect achievement of goals set.
- Regular progress reports should be submitted to the steering committee.

1.4 User requirements

- Business Analysts should carefully determine and document all user requirements relating to the system e.g. input, procedures, calculations, output, reports, financial reporting requirements, audit trails.
- Special care should be taken to consult both internal and external auditors as to their requirements & their recommendations concerning internal controls e.g. access controls, validation checks.
- Management of each user department should sign their approval of the specifications recorded to satisfy the needs of their individual departments.

1.5 Systems specifications and programming

- Program specifications should be clearly documented.
- Programming should take place in accordance with standard programming conventions & procedures e.g. for coding, flow charting, program routines.
- Programmers should carry out all program development in a development environment & should have no access to the live environment.

1.6 Testing

- Program coding of individual programs should be tested by the programmers using standard debugging procedures like program code checking and running the program with test data.
- The system should also be tested as a whole to ensure that all programs are integrating properly.
- The system should also be tested on an output level by management, users and auditors to establish whether the system is satisfying the requirements of its users.

1.7 Final approval

- Results of testing should be reviewed by all involved to ensure that necessary changes have been made and errors corrected.
- The project team should then obtain final approval from the board, users, internal audit and IT personnel before going ahead with conversion procedures.

1.8 Training

- A formal programme should be devised setting out in detail all personnel to be trained, dates & times for their training & allocating responsibility for training to specific, capable staff.

- ➢ User procedure manuals & updated, clearly defined job descriptions should be compiled & used in the training exercise.

1.9 Conversion

- Controls are necessary at this stage to ensure that programs & information taken onto the new system are **complete**, **accurate** and **valid**:
-
    - ➢ **Conversion project**: the conversion should be considered as a project in its own right.
    - ➢ **Data cleanup**: data to be converted must be thoroughly checked & discrepancies resolved prior to conversion. For example, if a new inventory application is being introduced; physical inventory should be counted so that correct quantities can be entered onto the system.
    - ➢ **Conversion method**: the conversion method must be selected:
        - parallel processing of the old & new systems for a limited period; or
        - immediate shut-down of the old system on implementation of the new system; or
        - conversion of the entire system at one time; or
        - phasing in different aspects over a set period
    - ➢ **Preparation & entry**: controls over preparation & entry of data onto the new system should include the use of a data control group to:
        - perform file comparisons between old & new files & resolve discrepancies;
        - reconcile from original to new files using **record counts** and **control totals**, e.g. if there were 300 employees on the old payroll, there must be 300 employees on the new payroll;
        - follow up exception reports of any problems identified through use of programmed checks e.g. no employee identity number;
        - obtain user approval for data converted in respect of each user department;
        - obtain direct information from customers or suppliers of balances reflected on the new system

1.10 Post-implementation review

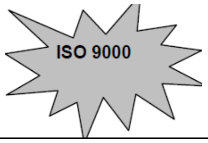
Users, IT personnel & auditors should review the system several months after implementation to determine whether:

- ★ the system is operating as intended;
- ★ the systems development exercise was effective;
- ★ all aspects of the new system are adequately documented in accordance with predetermined standards of documentation.

1.11 Documentation

- ➢ The project itself and all the activities which took place in the planning & execution of the project should be documented.
- ➢ Documentation relating to the system itself, must also be prepared, e.g. systems analysis, flowcharts, programming specifications, etc.
- ➢ Documentation should be backed up on an ongoing basis and stored offsite.

The following table provides examples of all the types of controls that should be put into operation for the in-house development & implementation of systems:

Controls for the in-house development and implementation of systems	Explanation of the principle with reference to an example
Standards 	Systems development must be subject to the ISO 9000 standards. ISO 9000 is a series of standards for quality management systems that is maintained by the International Organization for Standardization
Project approval 	A cost versus benefits study must be carried out, for example: Option 1: Cost of an existing system purchased directly from the developer: R5 000. Option 2: Cost of developing the system in house: R10 000. If the benefits offered by the different options are the same, it would be best to choose option 1.
Project management 	A project management team responsible for drawing up a project plan should be formed. This project plan should include the following: objectives, responsible persons, deadlines etc. The project management team is responsible for planning and controlling the project, and monitoring progress.
User requirements 	Multi-level involvement is necessary. All persons responsible for the system (e.g. users) should provide input.
Systems specifications and programming 	There must be agreement on the specifications before a system is developed. A computer language should be chosen, for example, as well as the symbols and abbreviations that will be used. This is followed by the programming, in other words, the physical writing of the programs.
Testing 	It is important that system development should precede the implementation of the system. The following kinds of tests could be carried out: ★ Program test: Tests the processing logic of a single program, in other ★ Words it tests whether the program could deal with every possible situation. ★ String test: A series of related programs is tested in order to determine whether the data is being correctly transmitted from one program to the next ★ Systems test: This test determines whether all the programmes in the system are interacting correctly. Test data is entered on the system to test whether the system handles it correctly ★ User acceptance test: The system is tested at an output level by management, the users and the auditors.
Final approval 	All the parties involved in the testing should finally approve the system before it is implemented. It is important that the system should be adapted and corrected to deal with the errors that showed up during testing.

Training 	A training programme that gives details of the people to be trained, the dates and times of training etc should be devised. Procedure manuals for users should be updated and used during the training sessions.
Conversion 	There are several steps that should be followed when converting a system: Development of a conversion project, cleaning of data, choice of a conversion method and lastly the preparation and physical entry of data. Controls over the preparation and input of data into the new system involve the following: ★ Compare old and new files – when a debtors' system is converted, for example, it is necessary to ensure that the same number of debtors' files exist before and after the conversion. ★ Reconcile original files with the new files with the aid of control totals – eg the sum of the outstanding debtors before and after conversion should be R50 890. ★ Print exception reports if certain conditions are not complied with – eg the number of inventory items transferred to the new system may not contain a negative value. If a negative value occurs, it would appear on an exception report. ★ User approval must be obtained from each department involved in data conversion eg the creditors section would give their consent if they were satisfied with the accurate, valid and complete transfer of creditors information and balances from the old to the new system. ★ Obtain direct evidence from customers and suppliers eg all customers and suppliers could be contacted to determine whether the outstanding balance as reflected on the new system is correct.
Post-implementation review 	A few months after the new system has been adopted, a post-implementation review should be carried out to measure the satisfaction of users, information technology personnel and auditors.
Documentation 	The project and all related activities should be documented. In addition, documentation relating to the system should also be prepared. This documentation should be regularly backed up and stored offsite.

Activity:

Systems testing, which takes place during the systems development phase, is an important measure for both the management of the entity and the auditors because it affords the last opportunity to test the system before it is implemented.

Write down (in point form) the objectives of system testing during the systems development phase.

Feedback:

The objectives of system testing during the systems development phase are to:

★ Determine whether the system is operating in accordance with its design specifications

★ Determine whether the operation of the system complies with user requirements

★ Determine whether all application controls are operating as they were designed to do

★ Demonstrate that correct input leads to correct output

★ Demonstrate that incorrect input, processing or output will be detected

Activity:

During the systems development phase, when conversion takes place from one system to another, controls are required since errors can arise when master and transaction files are converted to a new system. Such errors can arise when data in a record is accidentally changed or lost, or when records are omitted.

Describe the conversion controls applied during systems development that should detect or prevent errors during systems development when conversion to a new system takes place.

Feedback:

Conversion controls:

★ Approval for the conversion of files should be given before the conversion process begins. The purpose of this approval is to ensure that the files that are converted have been thoroughly checked.

★ The original and the new files must be reconciled by means of record counts, hash totals and financial totals.

★ Sections of the records from the original files can be compared with the corresponding sections of the records in the new files to make certain that there are no differences.

★ Requests for confirmation can be sent to third parties such as customers and users, who can be asked to check the information in the documents and correct it if necessary.

★ Exception reports can be used to detect and correct irregularities.

★ Operating approval must be obtained from the users after they have used the system a few times. Approval indicates that they are satisfied with the way the system is operating.

2. Systems development and implementation based on packaged software

When a company decides that it needs a new system, one of the options it has, is to purchase packaged software as opposed to developing the software itself (in-house). This is not just a matter of buying a package, installing it & away you go – the majority of the systems development & implementation controls will apply. The major difference between in-house developed and packaged software is that for purchased packages, the company will have no control over the specifications & development, e.g. writing the programs, or testing of the software. Purchased packages are designed to meet the generic requirements for lots of users with similar needs & although current packages contain hundreds of features & capabilities, the user basically gets what the package offers, nothing more and nothing less. This means that from the company’s perspective, the emphasis will be deciding whether the package offers features and capabilities which match with what the company’s users want.

2.1 The **advantages** of packaged software:

- ★ lower cost;
- ★ the entire software development project is completed far quicker because development & testing have been done on the software by the developers;
- ★ the package can be demonstrated up front, so IT personnel & users can see what the package "can do". Sample reports can be examined & the computer capabilities required by the software can be determined & tested;
- ★ technical support (by phone or over the internet) is usually available from individuals who are very skilled & knowledgeable about the specific package, and comprehensive manuals are supplied;
- ★ software companies usually upgrade the packages on an ongoing basis

2.2 The **disadvantages** of packaged software:

- ★ the package may not meet the company's requirements exactly
- ★ excellent software developed overseas may, for example, not satisfy South African tax or financial reporting requirements;
- ★ changes can't be made by a purchaser of the software

2.3 Summary of controls for the acquisition and implementation of packaged software

- ★ ***Project management*** – the entire exercise should be run as a project by a team appointed by the steering committee
- ★ ***Project approval*** – a feasibility study must still be conducted to determine:
  - ✓ user needs
  - ✓ specifications (capabilities, functions, controls) of packages available in the market;
  - ✓ costs and benefits;
  - ✓ technical support & reliability of the supplier
- ★ ***Approval*** – for the package chosen should be obtained from users, internal audit & the steering committee, and authorization for its purchase should be obtained from the CIO and the board.
- ★ ***Training*** – all affected IT personnel & users should be trained in the use of the new software.
- ★ ***Conversion*** – moving data onto the new system should be controlled.
- ★ ***Post implementation review*** – again IT personnel, users, internal audit, should review the new software several months after implementation to determine whether it is operating as intended.
- ★ ***Documentation*** – the systems documentation, user manuals, etc., will come from the supplier but the planning & execution of the project itself should be documented.

Study Unit 3.3

Access Controls

It is essential to control access in order to prevent damage to and the theft of equipment, as well as the manipulation, destruction or theft of data. Access controls should be designed to ensure that only authorised users obtain access to the computer facilities and data.

Access to all aspects of the system must be controlled:

a) hardware
b) computer functions at system level (accessing the computer system itself)
c) computer functions at application level (accessing a specific application or module)
d) data files / databases
e) utilities
f) documentation (electronic or hard copy)
g) communication channels

Security policy

1. **Least privilege**: employees should only be given access to only those aspects of the system which are necessary for the proper performance of their duties, e.g. a clerk in the wages department should not be given access to inventory records as he does not "need to know" what is contained in the inventory records.

▪

2. **Fail safe**: if a control "fails", whatever is being protected by that control, should remain "safe", e.g. if logical access control software malfunctions, the system should shut down completely, rather than allowing uncontrolled access.

▪

3. **Defense in depth**: this means that protection is not left up to one control only, but rather to a combination of controls

▪

4. **Logging**: the computer's ability to log (record) activity which takes place on it, should be extensively incorporated, e.g. unsuccessful attempts to access the system should be logged & followed up. Logging is **not** an effective control activity, **unless** the logs are regularly **and** frequently reviewed and follow up action taken where control violations are identified.

▪

The following table illustrates the principles of a security policy by means of examples:

Principle	**Explanation of the principle with reference to an example**
Least privilege	The foreman of the store should not have access to the debtors system since his duties do not include any aspects of the use of the debtors system.
Fail safe	If the internal controls detect irregular access to the inventory system, the system should be locked and no further functions/changes to the inventory system should be allowed.
Defense in depth	A number of controls rather than a single control should be implemented to protect the

	inventory system. For example: access to the inventory system can only be obtained from computers situated in the inventory section; only certain users can gain access to the system by means of passwords and, lastly, various modules of the computer system can be restricted by giving certain users reading rights only.
Logging	At the end of every week management should study the logging register. All unsuccessful attempts to gain access to the inventory system should be studied and followed up.

Physical access control

A combination of the following physical controls can be implemented to prevent unauthorized entry to an IT data centre. For example, the IT department as a whole could be contained in a separate building or wing of a building. All IT personnel would have their offices in this building. The building would also have a **dedicated room** in which all the equipment which runs the system would be housed, e.g. CPU, servers, routers, to run the company's systems. This dedicated room would be the data centre. Access to the IT building may be controlled & further access to the data centre itself would be far more strictly controlled. Only a limited number of personnel need access to the data centre itself whilst many more need access to the IT department.

★ **Visitors from outside the company to the IT building should**:

- be required to have an official appointment to visit IT personnel working in the IT department, e.g. external maintenance personnel;
- on arrival, be cleared at the entrance to the company's premises e.g. by a phone call to the IT department;
- be given an ID tag & possibly escorted to the department;
- not be able to gain access through the locked door (must "buzz");
- wait in reception for whoever they have come to see;
- be escorted out of the department at the conclusion of their business

★ **Company personnel other than IT personnel**

- there should be no need for other personnel to enter the ***data centre*** & access to the IT department should be controlled in a practical manner as there will be contact between the IT department staff & users on a regular basis

★ **Physical entry to the data centre**

- only individuals who need access to the data centre should be able to gain entry ;
- access points should be limited to one;
- access should be through a door which is locked other than when people are entering or exiting;
- the locking device should be de-activated only by swipe card, entry of a PIN number, scanning of biometric data, e.g. thumbprint;
- entry/exit point may be under closed circuit TV

★ **Remote workstations / terminals**

- terminals can be locked and secured to the desk;
- terminals must be placed where they are visible & not near a window;

- offices should be locked at night & at weekends

Logical access controls

Logical access controls will be primarily **preventive**, i.e. designed to prevent unauthorized access via terminals, but these will be supported by logs which are **detective**.

The following controls in various forms can be implemented through the access control software & other programs:

★ **identification**:
- user identification (user IDs)
- magnetic card or tag
- biometric data (e.g. thumbprint, facial recognition)
- terminal identification (system recognizes terminal ID number or name)

★ **authentication**:
- entering a unique password;
- entering a piece of information which an unauthorized individual would not know about the genuine user, e.g. great grandmother's first name;
- connecting a device to the USB port of the terminal (e.g.: dongle). A one-time password can be generated on a server & sent by SMS to the user. A combination of the above techniques is called multi-factor authentication & is used where very strict access control is required. The dongle will only work on a terminal on which the bank's specific software has been loaded, this is a form of terminal authentication

★ **authorization** (this is defining the levels of access to be granted to users and computer resources)
- once the system has authenticated the user, access will only be given to those programmes to which the user is **authorized** to have access
- a user may be granted read only; or
- read & write
- although modern software concentrates access privileges around the user, specific terminals can be linked to specific applications e.g. warehouse terminal not linked to the wage application, or to the EFT facility;
- restricted hours of operation, e.g. terminal shuts down at 4pm and comes on at 7am

★ **logging**
- this is recording access and access violations for later investigation. Logging and follow up is a detective control.

★ **Access tables**

The computer cannot perform logical access control unless a large number of details are defined in tables to which the system can refer. These tables identify all "objects" and "conditions" which the computer has to "know" in order to be able to control access. These objects include:
- all authorized PCs (PC IDs);
- all authorized users (user IDs);
- all passwords;
- all programs;
- all possible modes of access (no access, read-only, read and write), time of day

Access profiles are usually set up for “user groups” rather than for individual users, as this is a more efficient way of controlling access.

★ **Controls over passwords**

The strict control of passwords is fundamental to successful, logical access controls:

- passwords should be unique to each individual;

▪

- passwords should consist of at least six characters, be random not obvious, and a mix of letters, numbers, upper/lower case and symbols;

▪

- passwords / user-ID’s for terminated or transferred personnel should be removed /disabled at the time of termination or transfer;

▪

- passwords should be changed regularly & users should be forced by the system, to change their password;

▪

- the first time a new employee accesses the system, he / she should be prompted to change his initial password;

▪

- passwords should not be displayed on PCs at any time, be printed on any reports or logged in transaction logs;

▪

- password files should be subject to strict access controls to protect them from unauthorized read and write access. Encryption of password files is essential;

▪

- personnel should be prohibited from disclosing their passwords to others and subjected to disciplinary measures should they do so;

▪

- passwords should be changed if confidentiality has been violated, or violation is expected;

▪

- passwords should not be obvious, e.g. birthdays, names, name backwards, common words, and should not be the same as the user ID

▪

Other access control considerations

1. **Data communication**

Data communication relates to the transmission of information from a sender to a receiver in electronic form. Information must be sent down a link which may be a **fixed line**, e.g. a public telephone network, or a dedicated line linking two computers, or a **fibre optic** cable, or by **wireless** technology, e.g. satellite transmission, cellular telephones or even cordless computer devices, such as a cordless mouse.

Control is achieved by:

a) The implementation of specialized software which is responsible for:

- controlling access to the network;
- network management;
- data & file transmission;
- error detection and control;

- data security

b) encryption (converting data into a secret code)
c) the protection of physical cabling

2. **Firewalls**

Once a company's network is connected to an external network such as the internet there is an increased risk of unauthorised access to the company's network. A firewall is a combination of hardware & software that sits between the company's network & the external network, and is access control gateways which restrict what traffic can flow in and out.

3. **Libraries**

In a computer environment, libraries may be both in electronic form and in physical form. Library software will protect backup copies of programmes from unauthorised changes being made, record (log) any authorized access, audit changes and monitor user.

4. **Root access / system wide access / super-user privileges**

This level of privilege gives the user virtually unlimited powers to access and change, without trace, all programs & data, bypassing normal access controls and therefore should only be given to a very limited number of IT personnel.

5. **Utility programs / Database access**

Access to utility programmes & high level access directly to the database provides the potential to change / delete data & programs without leaving an audit trail.

Two categories of access controls are involved, namely physical and logical access controls. The distinction between these two categories is as follows:

Physical access controls are controls that are visible. For example, you can see a security guard standing in front of the gate of the electronic data processing section and you know that he will only allow you to enter if you sign a register.	
Logical access controls are controls that are built into the computer. When you log onto the computer, the system tests to see whether you are a registered user.	

Activity:
Explain what you understand by the encryption of data.

Feedback:
Encryption is the coding of data to disguise its meaning. The original data can only be recovered by the person or device that has the key required for decoding.

Continuity of Operations

These controls are aimed at protecting computer facilities from natural disasters (e.g. flooding or fire), as well as from acts of destruction, attack or abuse by unauthorised people. Our high crime rate and general unrest, places businesses at risk of armed robbery & damage from explosion.

1. Risk assessment

The dependence by large companies on their IT systems is huge & failure to assess & address IT risk threatens the continuity of operations. The auditor will evaluate whether:

- ★ assessing IT risk is an integral part of the company's risk assessment procedures;
- ★ there is an appropriate level of experience & knowledge with regard to IT risk on the risk assessment committee;
- ★ the risk committee meets regularly but is available to deal with the threat of unexpected IT risk on an ongoing basis;
- ★ the risk assessment committee recognizes & assesses all types of threat relating to IT which could disrupt operations including, e.g.:
  - fraud & theft perpetrated through the IT system;
  - physical and infrastructure damage;
  - hacking & viruses;
  - non-compliance with IT laws, rules, standards & best practice
- ★ accepted risk assessment protocols (way of doing things) are followed;
- ★ assessments are documented & reported to the board;
- ★ responses to risks are recorded, implemented and monitored

2. Physical security

These controls are designed to **protect** facilities against natural & environmental hazards & attack or abuse by unauthorized people. The following pertain more specifically to the **data centre**:

- ★ Physical location (site selection)
  - the data centre (and obviously the building in which it is housed), should be placed away from obvious hazards e.g. river banks, main traffic areas, the factory, stores of hazardous materials;
  - the facility should be located within a secure area within a building i.e. no outside walls & windows;
  - there should be a secure door & access control devices
- ★ Fire and flood
  - automatic gas release (e.g. CO2), smoke detectors, fire extinguishers, no smoking allowed;
  - situated above ground level and away from water mains;
  - raised flooring in the computer room
- ★ Power surges
  - use of "uninterrupted power supply" equipment & backup generators, particularly if continuity is critical (normally is)
- ★ Heat and humidity
  - air-conditioning preferably on its own electrical circuit

- Physical access controls

The following table provides examples of continuity of operations controls:

Continuity of operations controls	Explanation of the control with reference to an example
Physical location 	As a result of large-scale expansion, management is currently building other facilities. Despite the high cost implications, management has decided not to locate the building in an industrial area. The reason is that the increase in the emission of smoke and exhaust gases in industrial areas can damage the computer equipment.
Fire and flood 	Management has decided to install fire detection equipment in the building. The sensors are sensitive to smoke and heat and would activate an alarm immediately if a fire were to break out.
Power surges 	Large-scale power failures have a negative effect on the productivity of computer operators. Management was therefore compelled to buy back-up generators.
Heat and humidity 	The life of computer equipment can be shortened if it is placed in an area that gets very hot. Management therefore decided to install air-conditioning units to maintain a constant temperature in the computer room.
Access controls 	See study unit 3.3

3. **Disaster recovery**

There are controls implemented to minimize disruption as a result of some disaster which prevents processing & destroys / corrupts programmes & data.

a) **A disaster recovery plan**:

- a written document which lists the procedures which should be carried out by each employee in the event of a disaster;
- the plan should be widely available so that there is no frantic searching if a disaster occurs. Time is usually precious;
- the plan should address priorities i.e. the order in which files or programmes should be reconstructed, with the most important being allocated the highest priority, as well as where backup data, programmes, hardware, etc. may be obtained;
- the plan should be tested;

- ★ the plan should be detail alternative processing arrangements which have been agreed upon in the event of a disaster, e.g. using a bureau

b) **Backup strategies**:

- ★ backups are copies of all or parts of files, databases, programmes taken to assist in reconstructing systems or information, should they be lost or damaged;
- ★ backup of all significant accounting and operational data and programme files should be carried out frequently and regularly;
- ★ at least three generations of backups should be maintained (grandfather, father, son);
- ★ the most recently backed up information should be stored off-site;
- ★ all backup should be maintained in fireproof safes & on-site backups should be stored away from the computer facilities;
- ★ critical data and programs can be copied in real time to a “mirror site”, so that it is possible to switch processing to the mirror site in the event of a disaster e.g. a large refinery in CPT duplicates its processing on a second computer installation housed in a separate, very secure (bomb proof as well) site on the premises;
- ★ copies of all user and operations documentation should be kept off-site

An example of an effective disaster recovery plan (of ABC (Pty) Ltd) is given below.

- ➢ The disaster recovery plan was documented during the establishment of ABC (Pty) Ltd. This plan sets out detailed procedures and is revised and updated annually.
- ➢ The updated disaster recovery plan is issued to all members of staff annually. It is also stored at a central point on the network.
- ➢ The disaster recovery plan covers the following areas:

- sequence in which files and programs should be reconstructed
- staff responsible for the reconstruction procedures
- location of the back-up data
- names and telephone numbers of suppliers who could provide assistance
- alternative processing methods such as the manual processing of transactions

- ➢ After the annual updating of the disaster recovery plan it is tested to ensure that it is feasible

Activity:
Explain what you understand by the concept “mirror site”.

Feedback:
During the updating and processing of critical data and programs they are automatically copied to a “mirror site”. If there is a disaster - suppose a fire has wiped out all critical data and programs - it would be possible to continue with data processing on the “mirror site.”

4. **Other measures**

There are a number of other control measures that can be taken which will assist in preventing or alleviating disaster:

- ★ applying the concept of redundancy;
- ★ regular maintenance and servicing of equipment to prevent failure;

★ adequate insurance cover to provide funds to replace equipment;

★ avoidance of undue reliance on key personnel by maintaining complete and appropriate documentation & by training of understudy staff, e.g. the disaster recovery plan should not revolve around one staff member;

★ arrangements for support to be provided by suppliers of equipment & software, who may even provide alternate processing facilities;

★ the use of fire walls & use of anti-virus software

System Software and Operating Controls

System software controls are aimed at monitoring the system. Operating controls are the policies and procedures which should be in place to work with the system software controls to make sure the computer system run like a “well-oiled machine”.

System software is made up of various kinds of software including, i.e:

1. **Operating system software which**:
   - controls the use of the hardware
   - tests critical components of the hardware & software where the computer is started
   - controls the input and output of data
   - schedules the use of resources and programmes
   - monitors the activities of the computer and keeps track of each programme & the users of the system
   - provides the interface with the user, e.g. how the user communicates with the computer

2. **Network management software**:
   - which enables computer systems to communicate with each other

3. **Database management software**:
   - which enables the user to create, maintain & use data files in an efficient & effective manner

4. **System development software**:
   - which is used to develop new software, e.g. assemblers, compilers

5. **System support programmes**:
   - such as anti-virus software, data compression software, etc

Controls include:

- ★ Operating policies & procedures which are fully documented, regularly reviewed and updated
- ★ System software which maintains a log of activity on the system detailing all activity which has taken place, including:
  - Hardware malfunction
  - Intervention by personnel during processing
- ★ Skilled technicians who can resolve operating problems for users
- ★ Adherence to international system software control protocols (how things are properly done)
- ★ Follow up on access violations, attempted violations
- ★ Follow up of potential virus infection
- ★ Adherence to manufacturers’ equipment, maintenance & usage guidelines
- ★ Strict supervision and review of IT employees (IT manager needs to know what his staff are doing)

The following table provides two examples of kinds of operating controls that should be instituted:

Operating control	Explanation of the control with reference to an example
Equipment operation and maintenance 	Hardware must be operated and maintained according to the manufacturer's instructions. For example, computers should not be switched off at the plug.
Machine servicing 	Like motor cars, machines must be serviced regularly. A photocopier must be serviced every 3 months, for instance.

Documentation Controls

Documentation

Sound document policies are essential, because documentation can be critically important in:

- ★ improving overall operating efficiency;
- ★ providing audit evidence in respect of computer related controls;
- ★ improving communication at all levels;
- ★ avoiding undue reliance on key personnel;
- ★ training of users when systems are initially implemented

There are two major objectives to bear in mind regarding documentation:

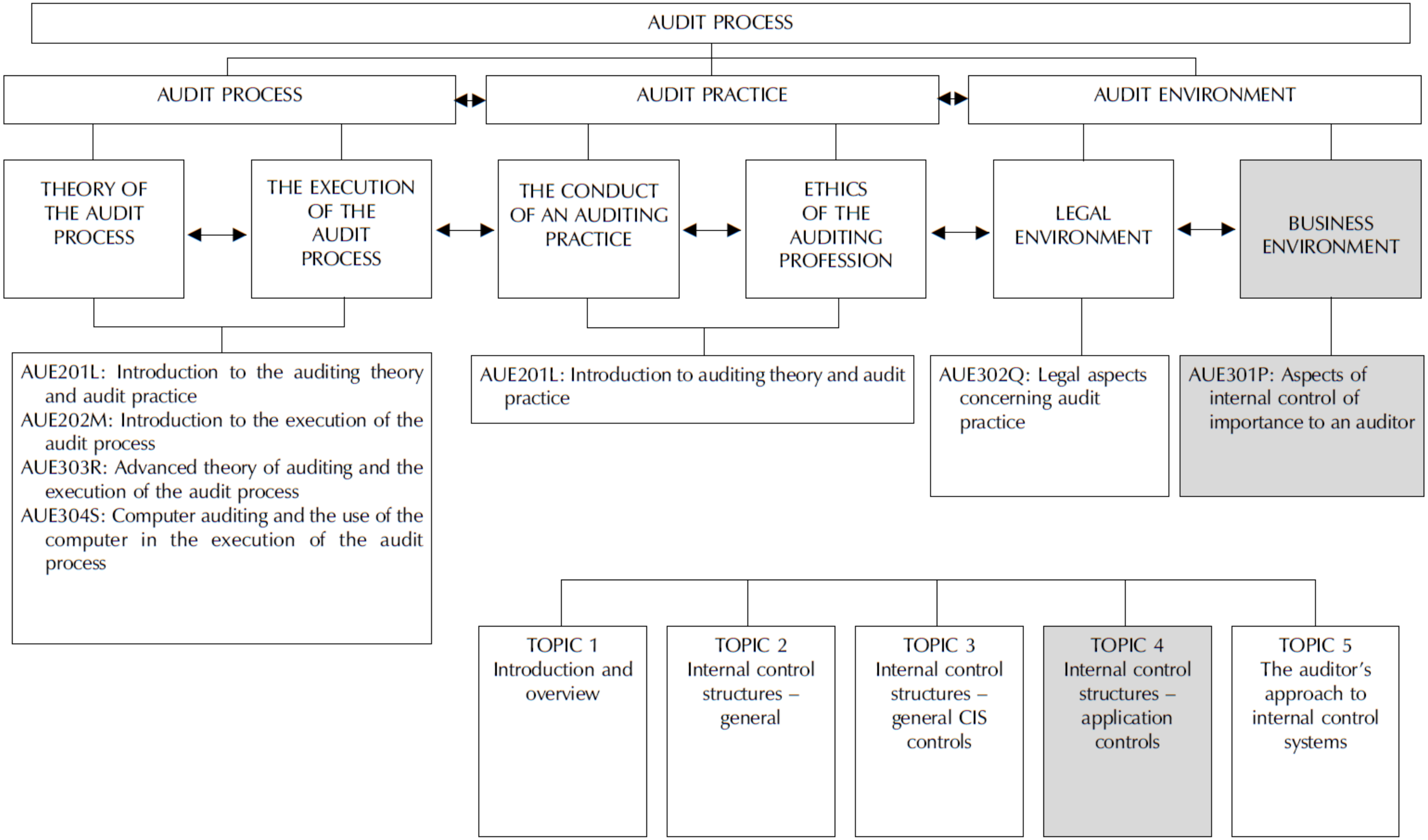
- ★ all aspects of the computer system should be clearly documented;
- ★ access to documentation should be restricted to authorized personnel

Documentation standards

Pre-determined standards should exist for documentation and adherence thereto should be enforced. These standards should require at least:

- ★ general systems descriptions;
- ★ detailed descriptions of program logic;
- ★ operator and user instructions including error recovery procedures;
- ★ back-up & disaster recovery procedures;
- ★ security procedures / policy;
- ★ user training;
- ★ implementation and conversion of new systems

SCHEMATIC REPRESENTATION OF THE SUBJECT OF AUDITING



AUDIT PROCESS

AUDIT PROCESS

AUDIT PRACTICE

AUDIT ENVIRONMENT

THEORY OF THE AUDIT PROCESS

THE EXECUTION OF THE AUDIT PROCESS

THE CONDUCT OF AN AUDITING PRACTICE

ETHICS OF THE AUDITING PROFESSION

LEGAL ENVIRONMENT

BUSINESS ENVIRONMENT

AUE201L: Introduction to the auditing theory and audit practice
AUE202M: Introduction to the execution of the audit process
AUE303R: Advanced theory of auditing and the execution of the audit process
AUE304S: Computer auditing and the use of the computer in the execution of the audit process

AUE201L: Introduction to auditing theory and audit practice

AUE302Q: Legal aspects concerning audit practice

AUE301P: Aspects of internal control of importance to an auditor

TOPIC 1
Introduction and overview

TOPIC 2
Internal control structures – general

TOPIC 3
Internal control structures – general CIS controls

TOPIC 4
Internal control structures – application controls

TOPIC 5
The auditor's approach to internal control systems

Internal Control Structures – Application Controls

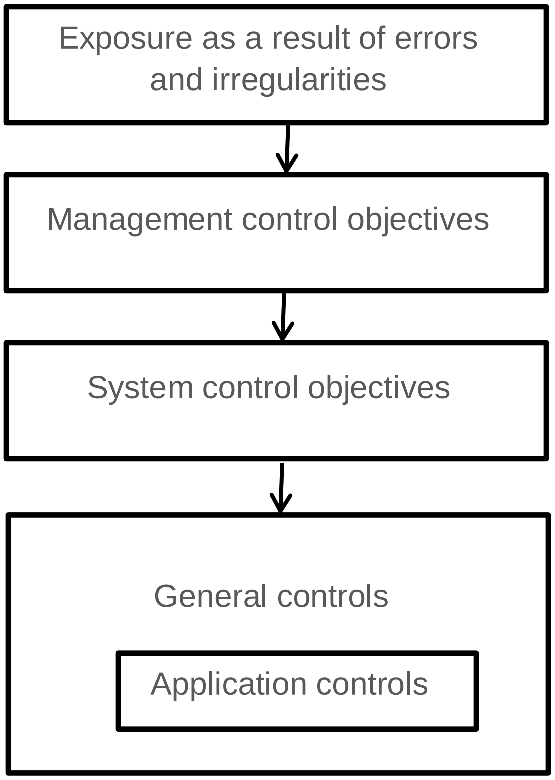
Application controls are user and programmed controls and are embedded in each of the data processing functions, namely input, processing and output.

Application controls must ensure the following:

- ★ only valid transactions are processed, and they are completely and accurately processed and recorded
- ★ data in accounting and supporting files are kept properly up to date
- ★ assets are protected against physical loss or theft

Controls	Definition	Example
User controls	Controls performed manually by the users	• checking of exception reports • authorization of transactions
Programmed controls	Controls embedded in the application program code and applied by the computer	• limit tests • alphanumeric tests

The place of application controls in an internal control system can be schematically represented as follows:


Exposure as a result of errors and irregularities
Management control objectives
System control objectives
General controls
Application controls

Systems objectives are achieved by using general and applications controls that prevent, detect and correct errors in every phase of the transaction cycle. Application controls are specifically instituted for each individual accounting application. General controls create the environment within which the application controls operate.

Auditors approach:

a) if general controls & application controls **cannot** be relied upon – substantive testing
b) if general controls **cannot** be relied upon but application controls **can** be relied upon – substantive testing
c) if general controls **can** be relied upon but application controls **cannot** be relied upon – substantive testing
d) if general controls & application controls **can** be relied upon – control testing

The relationship between controls and systems objects is characterised by the prevention, detection and correction of errors.

Preventive measures prevent errors.

Detection measures were designed to pick up unavoidable errors (errors that occur in spite of effective preventive measures).

Corrective measures ensure that errors that are detected can be properly corrected and the data resubmitted for input and processing.

Application Controls

1.1 An **application** is a set of procedures and programmes designed to satisfy all users associated with a specific task, e.g.: the payroll cycle. Other examples include making sales, placing orders with suppliers & receiving or paying money.

▪

1.2 An **application control** is any control within an application which contributes to the accurate & complete recording and processing of transactions which have actually occurred, and have been authorized (valid, accurate and complete information)

▪

1.3 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.

▪

1.4 Controls must be implemented over **masterfiles**. A masterfile is a file which is used to store only standing information and balances

▪

1.5 The objective of controls in a computerized accounting environment is generally regarded as being centred around the occurrence, authorization, accuracy and completeness of data and information processed b y and stored on the computer.

-
- **Occurrence** and **authorization** is 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 authorized by management

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

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

Understanding control activities in a computerized accounting system

2.1 Introduction

User controls are also called manual controls and they include all the controls which people carry out, e.g. signing a cheque.

2.2 Segregation of duties

Segregation of duties in a computerized environment is achieved by controlling access which employees have to the system itself, the application on it, and the modules or functions within the application. This is achieved by setting up user profiles on the system for each employee which detail exactly what that employee must be given access to and what he can do when he has access, e.g. read a file, write to a file, make an enquiry, authorize a transaction, etc.

2.3 Isolation of responsibilities

In a manual system, this is achieved by making a specific employee responsible for each function or procedure and requiring that the employee sign a document to acknowledge having carried out the procedure.

A computerized system can enhance isolation of responsibility by programming the computer to produce a log of who did what and when they did it. Access controls also contribute to isolation of responsibility. Passwords can also restrict (isolate) access.

2.4 Approval and authorization

Approval and authorization can be a user (manual) procedure, e.g. signing a document, or an automated (programmed) control. In a computerized system the authorization and approval of a transaction can be carried out far more effectively and efficiently than in a manual system. For example:

- ★ an order clerk who wants to place a purchase order with a supplier who is not approved by the company, will be prevented from doing so because the system will not allow an order to be initiated on the system if the supplier is not on the approved supplier (creditors) masterfile.

A computerized system is very effective at **preventing** unauthorized transactions from taking place. It is certainly true that these kinds of controls can be overridden, but overrides will be logged by the computer and should be followed up. Logging and follow up is a detective control.

Another advantage or approval on the system is that the parties involved do not have to be geographically close.

One potential risk with regard to approval / authorization in a computerized system is that the initiation and execution of transactions may be automatic with no visible or actual authorization of the transaction, e.g. the rate of interest paid on a savings account at a bank, or the rate of interest charged on a debtor's account by a company, may automatically increase when the savings balance reaches a specified amount or the debt has been outstanding for a specified period of time.

2.5 Custody

In the case of **cash in the bank**, the company does not have physical control over the cash, but must control unauthorized removals from its bank account. In a manual system, this will be done by controlling the company cheque book itself, limiting signing powers to senior officials (preventive controls) and reconciling the company's cash book with the bank statement (detective controls). In a computerized payment system, e.g. EFT for the payment of creditors and employees, far stricter controls must be implemented over access to the EFT facility and authorizing and releasing of funds.

2.6 Access controls

Access violations can have extremely serious consequences for the business. These include:

- destruction of data;
- "theft" of data;
- Improper changes to data;
- Recording of unauthorized or non-existent transactions

★ Access to particular applications can be restricted to particular terminals, e.g. the ability to affect an EFT transfer can be restricted to the terminal of the financial manager.

★ Access is restricted in terms of user profiles at both systems level and applications level, e.g.:
  - at systems level, access to a particular application may be restricted to particular users,
  - at application level, access to specific program functions may be restricted to particular users on the "least privilege" basis e.g. sales order entry is limited to telesales operator

★ PC time out or automatic shutdown will prevent continued attempts to access the system, as well as the threat of employees leaving their terminals unattended.

The "least privilege" principle may be implemented in a number of ways:

a) restrictions on access to a module or program function e.g. masterfile amendments;
b) restrictions in terms of mode (type) of access, e.g. read-only;
c) restrictions in terms of time of day (e.g. working hours only as in a bank or telesales call centre);
d) extent of access to data (e.g. allowing only restricted views of certain data so that sensitive data fields are hidden to users of lower privilege levels)

In effect a user:

- must **identify** himself to the system with a valid user ID;
- must **authenticate** himself to the system with a valid password;
- will only be given access to those programmes and data files to which he is **authorized** to have access to

2.7 Comparisons and reconciliation

A reconciliation is a comparison of two different sets of recorded information or of recorded information and a physical test. In a manual system this is done by employees laboriously comparing the two sets of information to identify differences. In a computerized system this reconciliation can be completed accurately, comprehensively and in no time at all.

Along with the ability for a good computerized system to produce any number of reports, including those which can be printed out and used for physical comparisons, its ability to instantly compare any data on the system makes comparison and reconciliation a valuable and effective control activity.

2.8 Performance reviews

These control activities include reviews and analysis of actual performance versus budgets, forecasts & prior period performance as well as relating different sets of data to one another. The huge advantage which a computerized system has is its ability to produce numerous useful reports, including comparisons, reconciliations and reasons for differences. For example, provided the necessary data is in the database, sales can be extensively analysed, reports can be generated to show what quantities or products are selling, which specific models or colours or sizes are most popular or are not selling, what gross profit is being generated from each sale, the region in which the products were sold, etc.

Batching

1. Batching
1.1 batch entry, batch processing / update
1.2 on-line entry, batch processing / update
1.3 on-line entry, real time processing / input

1. Batching

Batching is a technique which assists in controlling an activity which will be carried out on a batch of transactions with the intention of making sure that all the transactions in a batch are subjected to the activity.

Batching still has a place, for example in a wage system where up to date information is only needed at weekly intervals. The daily hours worked by each employee will be accumulated and then entered individually as items in a batch & processed in a batch. The following description of batching illustrates the principle of batching at the input stage:

★ Source documents are grouped into separate batches of say 50, and the following **control totals** manually computed:
  - **financial totals**: totals of any fields holding monetary amounts;
  - **hash totals**: totals of any numeric field e.g. invoice number;
  - **record counts**: totals of the number of records in the batch e.g.50
  -

★ A batch control sheet should be prepared and attached to each batch. The batch control sheet should contain:
  - a unique batch number e.g. batch 3 of 6, week ending 31/7/14;
  - control totals for the batch;
  - identification of transaction type e.g. invoices;
  - spaces for signatures of all people who deal with the batch e.g. prepared by:…., checked by:…., reviewed by:…..

★ A batch register should be used to record physical movement of batches; the register should be signed by the recipient of the batch after checking what is being signed for, e.g. transfer of the clock cards to the payroll department.

Note: Batching assists with the following:
- Identifying data transcription errors (e.g. incorrect values keyed due to transposition errors);
- Detection of data captured into incorrect fields;
- Detection of invalid (e.g. duplicate) or omitted transactions, e.g. if a clock card is entered twice

1.1 **Batch entry, batch processing / update**

★ Data is captured initially onto manually prepared source documents e.g. sales invoice.

■

★ These source documents are then collected into batches & entered via the keyboard with control totals in these batches. Relevant program checks take place as the information is keyed in e.g. validation check on employee number. The information is converted into machine readable form and held on a transaction file.

■

★ These transactions are then processed as a batch when it is convenient to do so and the relevant masterfiles are updated to reflect the effect of the entire batch on affected masterfile balances. Control totals before and after processing are compared.

■

★ Not common, particularly as it is slow and information is not up to date.

■

1.2 **On-line entry, batch processing / update**

★ Data is entered via a keyboard immediately as each transaction occurs, e.g. a sales order is placed by telephone & the operator keys in the details as the conversation with the customer takes place. Relevant program checks take place as information is keyed in.

■

★ The information is converted into machine readable form and held on a transaction file.

■

★ Control totals are created by the computer on the batch for the transaction file.

■

★ The transactions are then processed as a batch and the relevant masterfiles are updated to reflect the effect of each transaction in the batch on affected masterfile balances, e.g. they could be processed at the end of each day

■

★ Entry of the transaction is efficient, but information is not immediately up to date. The longer the period that the batch of transactions is not processed, the less up to date the information.

■

1.3 **On-line entry, real-time processing / update**

★ Data is entered via a keyboard immediately as each transaction occurs. Relevant program checks take place as information is keyed in.

■

★ The relevant masterfiles are updated immediately to reflect the effect of each individual transaction on affected masterfile balances, e.g. a seat booked on an airplane will instantly update the “seats available masterfile”.

■

★ Entry of the transaction is efficient & information is right up to date.

■

Activity:

The purpose of control totals in a CIS environment is to detect the loss of or non-processing of input documentation or data, or errors in data preparation.

Using examples, describe and illustrate three (3) different kinds of control totals that comply with the above requirements.

Feedback:

Explanation of control total	**Example**
Financial total: the total of a field containing a monetary value	Rand value of the sales represented by all the sales invoices in a batch
Hash total: a total calculated on any numerical field	Total of all the debtors' numbers of all the sales invoices in a batch
Record counts: the total of the number of physical records keyed in during data preparation	The number of sales invoices in a batch, eg 50

Screen Aids and Related Features

Screen aids have been classified as all the features, procedures and controls which are built in to the application software & reflected on the screen to assist a user to capture information accurately and completely, and to link the user's access privileges to the screen in front of him.

1. **Minimum keying in of information**

- The principle is that the less information that has to be keyed in, the less errors are likely to occur & the less time it takes, e.g.:
  - in a telesales system, the customer should be required to give only his account number or name which, when keyed in, will automatically retrieve all other standing details, provided the account number is valid.
  - techniques such as "drop down" lists which simply require the user to "select and click" the option they require from the options provided on the dropdown list.

2. **The screen should be formatted**

- The screen should be formatted in terms of what hardcopy would look like e.g. when entering an order from a customer the screen should look like the sales order, and should have easily recognizable fields into which data is entered such as a box with the letters QTY above it.

3. Extensive use of **screen dialogue and prompts**

- These are messages sent to the user to guide him, e.g. a prompt may appear on the screen reminding the user to confirm and re-enter a field.

4. **Mandatory fields**

Keying in will not continue until a particular field or all fields have been entered. Such fields may be hi-lighted in red or identified by a star or there may even be a prompt if the user misses out that field & moves on to the next field.

5. **Shading of fields**

Which will not react if "clicked on", e.g. an on-screen sales order may have the customer's account number & details shaded, the user completing the sales order will not be able to change these fields.

Programme Controls – Input and Processing

It is essential to design and implement controls around the **input of data** to ensure that the data that is entered to update masterfiles **occurred** and is **authorised**, **complete** and **accurate**.

If management neglects to design and implement controls for the input of data, the following errors are possible:

- ★ Unauthorised data could be entered
- ★ Input errors could occur;
- ★ Data could be lost during input;
- ★ Data could be added or modified during input;
- ★ Errors could occur when rejected data is corrected and re-entered.

It is also necessary to implement controls during **data processing** to ensure that only occurred and authorised, complete and accurate data is processed.

If management omits to design and implement controls for the processing of data, the following are among the errors that could occur:

- ★ Data could be lost during processing
- ★ Invalid data could be added during processing
- ★ Data could be modified during processing
- ★ Computational or accounting errors could occur

Programming controls – input and processing

Programme checks are controls which are built into the application software, with the intention of validating/editing information / data which is entered or processed. Validation can take place at the input and / or processing stages. Vast quantities of transactions can be subjected to a range of programmed controls to consistently produce reliable information. Errors are reduced and information is provided timeously.

1. Programme checks - input

a) **Existence / validity checks**

- ★ **validation checks** validate data keyed in against the masterfile e.g. a customer's account number will be checked against the debtors masterfile
- ★ **matching checks** amount to input being matched against data that is already in the database
- ★ **data approval / authorization checks** test input against a preset condition e.g. to make a sale on credit, a liquor store requires that the customer's identity number be entered on a computer generated invoice. If the customer is under 18 (which the identity number will indicate), a sales invoice cannot be generated (the sale is not authorized).

b) **Reasonableness and limit checks**

- ★ **limit checks** detect when a field entered does not satisfy a limit which has been set, e.g. the normal hours worked by an employee in a week cannot be entered at a quantity greater than 40 hours

- ★ **reasonableness checks** to accept the data being entered, must fall within reasonable limits when compared to other data, e.g. if a normal order from a customer for an inventory item is 100 units, and a clerk enters 1,000, the screen will display a message querying the entry, although there is no limit on the quantity ordered.

c) **Dependency checks**

An entry in a field will only be accepted depending on what has been entered in another field, e.g. the acceptability of entering a credit limit of R 100 000 on a debtors account will depend on the status allocated to the debtor. If the debtor's credit status rating is A+ (very good), the credit limit of R 100 000 will be acceptable. If the status is only B+ then the credit limit will not be acceptable.

d) **Format checks**

- ★ **alpha-numeric checks** prevent / detect numeric fields which have been entered as alphabetic & vice versa, e.g. when entering an employee's identity number, all digits must be numeric
- ★ **size checks** detect when a field does not conform to pre-set size limits, e.g. an identity number entered must have 13 digits
- ★ **mandatory field / missing data checks** detect blanks where none should exist, if a quantity is not entered in a quantity field on an internal sales order, data capture cannot continue
- ★ **valid character and sign checks**, the letters, digits or signs entered in a field are checked against valid characters or signs for that field, e.g. a minus sign (-) could not be entered in a quantity order field

e) **Check digits**

A check digit is a redundant (extra) character added to an account number, part number, etc. the character is generated by manipulating the other numerical characters in the account number. When the account number is keyed in, the computer performs the same manipulation on the numerical characters in the account number and if it has been entered (keyed in) correctly, the computer will come up with the same check digit which was added to the account number originally. If it does not match, the computer sends a screen message to inform the operator that the account number has been incorrectly entered. Check digits use up processing resources & therefore are limited to critical fields. They **cannot** be used on financial fields.

f) **Sequence checks**

Detect gaps or duplications in a sequence of numbers as they are entered, e.g. if numbered masterfile amendment forms are being keyed in, a sequence check will alert the user if there is a gap or duplication in the numerical sequence.

Where information is entered off a source document, the source document should be:

- ➢ Pre-printed, in a format which leaves the minimum amount of information to be manually filled in;
- ➢ Pre-numbered, sequencing facilitates identification of any missing documents;
- ➢ Designed in a manner which is logical and simple to complete & subsequently enter into the computer, e.g key pieces of information should have a prominent position on the document;
- ➢ Should be designed to obtain blank blocks which can be used for authorizing or approving the document;
- ➢ Unused source documents should be kept under lock and key by an independent person and a register of receipt and issue of the document kept.

2. Programme checks – Processing

Processing controls assist in ensuring that data is processed accurately and completely.
Processing will not normally stop if an error is discovered. The error will be written to an exception report.

a) **Programme edit checks**

- ★ **Sequence test** the sequence of documents processed is checked for gaps, e.g. after processing credit notes, the computer may identify missing credit note numbers
- ★ **Arithmetic accuracy check** e.g. reverse multiplication
- ★ **Reasonableness / consistency / range tests** after processing of a transaction has taken place, the result is compared by the computer itself to other information for reasonableness e.g. a wage of R 5000 is not reasonable for a grade 3 employee or compared to his prior week's earnings
- ★ **Limit test** identifies amounts which fall outside a predetermined limit after processing, e.g. credit sales to a customer have pushed the debtor's balance owing beyond the customer's credit limit
- ★ **Accuracy test**, where amounts are allocated to columns & the columns are independently cast (added up), the totals of the columns can be cross cast (added across) and compared to the total amount allocated e.g. net pay + paye + medical aid deduction = gross pay
- ★ **Matching** in the context of processing is about comparing data which has been processed, against data which is already in the database, e.g. a matching control may match clock cards processed with the employee masterfile to identify employees for whom there was no clock card information. The reason there is no clock card may be perfectly valid, e.g. the employee was on holiday for the week, but it could also be a processing error.

b) **Programme reconciliation checks**

- ★ **Control totals**, e.g. record counts, hash totals from input are compared to record count and hash totals after processing
- ★ **Run-to-run totals**, a final balance arrived at after processing is compared to the opening balance and individual totals of transactions e.g. the closing balance on debtors (31 May) is compared to the opening balance on debtors (30 April) plus the total of May sales (debits) less the total of May receipts (credits)

The reliability of **hardware** also plays an important part in processing. Modern computer equipment is very reliable, and the hardware will have its own range of hardware controls, e.g.:

- ★ **Parity checks**: a redundant bit is added to data to make the sum of the bits in the data concerned, even (even parity) or odd (odd parity). Changes in parity detected as a result of this check indicate that an error has occurred in transmission or processing.
- ▪
- ★ **Valid operation code**: the processor checks if the instruction it is executing is one of a valid set of instructions.
- ▪
- ★ **Echo check**: the processor sends an activation signal to an input / output device – that device returns a signal showing it was activated. Echo checks can also be used to detect corruption of messages in transit by bouncing the signal back from the recipient of the message to the sender so that the sender

can compare it against the original message for any errors, which may have occurred during transmission.

-

- ★ **Equipment check**: input / output devices are activated prior to a read / write operation to ensure they work correctly.

-

Activity:

Name and describe four types of built-in hardware controls with reference to suitable examples.

Feedback:

Built-in hardware controls	**Description**
Parity check	The computer adds a redundant bit to a field on the basis of the logical relationship between the characters that make up the field. If the field is sent from the computer to a printer, the printer recomputes the bit and compares it with the original bit attached to the field during processing. This ensures that the processed information is not altered during transmission to a printer.
Valid operation code	This test ensures that a computer will only carry out valid actions. During the processing of clock cards this test ensures that the number of hours is multiplied and not divided by the hourly wage rate.
Echo test	This is a test that ensures that information is correctly transmitted from one component to another. If the computer is processing wage cards, for example, and the information is sent to the printer, the printer will echo the information to the computer. The computer will then compare the information received from the printer with the information that was originally sent over.
Equipment test	This is a test carried out by the computer when it is switched on. This test determines whether all the components of the computer are present and are functioning correctly. For example, the computer would perform a test to determine whether the disc driver is functioning correctly.

Output Controls

The output of a data processing system can be stored in machine-readable form, visually displayed or printed on paper. Output controls mainly pertain to printed output, although control over visual display is also important.

The objective of output controls is to ensure that output is accurate and complete and that its distribution is strictly controlled, for example, confidential output does not go to the wrong individuals. Output does not have to be hardcopy; it can be “on screen”.

Controls over distribution will include preventive controls such as:

★ clear report identification

  ○ name of report

  ○ time and production number of report

  ○ processing period covered

  ○ sequenced pages and “end of report” messages

★ a distribution matrix of who is to receive which output and when. This should be aligned to the user profiles & access privileges so that individuals who do not need access to the report, etc, cannot access them on the system

▪

★ if output is hardcopy & printed out at a certain point and distributed to users, its movement should be controlled by the distribution list (who gets what and when)

▪

★ output which is confidential should be designed to promote confidentiality, e.g. “sealed envelope” salary slips

▪

★ confidential information for employees which is emailed to them (such as payslips) should not be emailed to their work PC’s

▪

★ output which is printed out, especially more sensitive information, should be printed out only in the departments which require the output, and if it is confidential, under the supervision of authorized personnel

▪

★ input which is not required should be shredded, not just left about or thrown away as a complete document

▪

User controls will include (all detective controls):

★ review of output for completeness e.g. numerical sequence check

▪

★ reconciliation of input to output e.g. foreman of each cost centre reconciles overtime worked with his factory overtime records

▪

★ review of output for reasonableness e.g. financial manager reviews, week-to-week wage reconciliations (payroll manager will conduct detailed tests on the week to week wage reconciliation produced by the system)

▪

- ★ review and follow up of any exception reports produced during processing e.g. individual wage payments which failed “reasonableness test” during processing
- ▪

Activity:

1. Describe how the “occurrence and authorisation” objective for output controls differs from the “occurrence and authorisation” objective for input and processing controls.
2. Describe the output controls over the distribution of documentation to users.

Feedback:

1. The “occurrence and authorisation” objective is changed to "correct and confidential distribution” because an important part of output control is to ensure that output is distributed to an authorised user.

2. **Controls to achieve the “occurrence and authorisation” objective for output controls:**
   - ★ Clear report identification practices must be implemented, for example:
     - the name of the report
     - the time and production number of the report
     - the processing period covered
     - sequenced pages
   - ▪
   - ★ Compilation of a distribution checklist, which identifies all the items of output and indicates who the authorised recipient of the output is.
   - ▪
   - ★ Recording of output in a distribution register to control movement. The recipient of the output must be asked to sign for receipt of the output.
   - ▪
   - ★ The print function for the printing of confidential information should be restricted to printers that are under the control of suitable officials.
   - ▪
   - ★ The design of stationery must promote confidentiality, for example salary slips should be of the “sealed envelope type”.
   - ▪
   - ★ Shredding of all output that is not required, such as by-products of the printing of confidential information, for example carbon paper.
   - ▪
   - ★ Confidential information for employees which is e-mailed to them should not be emailed to their work PCs.

Logs & Reports

Various logs and reports can be produced by the computer and either printed or accessed on screen. Access can be restricted to read-only and should be for all logs of computer activity which form part of the audit trail.

Types of logs and reports used may include:

★ **audit trails** – provide listings of transactions and summaries and lists of tables or factors used in processing

■

★ **run-to-run balancing reports** – which provide evidence that the opening balances which have been updated by a series of transactions have resulted in correctly calculated closing balances

★ **override reports** – which provide a record of computer controls which have been overridden by employees using supervisory or management privileges. Abuse of such privileges is a threat to the objective of validity

■

★ **exception reports** – which provide a summary listing of any activities, conditions or transactions which fall outside of parameters which have been set for control purposes, e.g. employees whose remuneration for the week falls outside the reasonableness parameters set for employees of that grade

■

★ **activity reports** – which provide a record for a particular resource, of all activity concerning that resource, e.g. names of users, usage times & duration of usage

■

★ **access / access violation reports** – particularly important in relation to sensitive applications such as electronic funds transfer and payroll

■

Study Unit 4.6

Masterfile Amendments (Masterfile Maintenance)

Masterfiles (which contain standing data and the latest balances) are an integral part of processing. If these files are not protected against unauthorised amendments, there is a possibility that the information generated by the processing may be invalid. The following are examples of masterfile amendments:

- A supplier is added to or deleted from the list of authorised suppliers
- The particulars of a member of staff are added to or deleted from the salaries masterfile

The application controls over masterfile amendments are very important. The objective will be that:

a) only valid (authorised) amendments are made to masterfiles
b) the details of the amendment are captured & processed accurately & completely
c) all masterfile amendments are captured & processed

Below is an example of the controls over a debtor's masterfile amendments:

Procedure	Application control and related comments
1. Record all masterfile amendments on a source document ■ ■ ■	1.1 All amendments to be recorded on hardcopy masterfile amendment forms MAFs (no verbal instructions) ■ 1.2 MAFs to be pre-printed, sequenced & designed in term of sound document design principles
2. Authorise MAF ■ ■	2.1 The MAFs should be: • Signed by two reasonably senior debtors personnel • Cross referenced to the supporting documentation
3. Enter only authorised masterfile amendments onto the system accurately and completely ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	3.1 Restrict write access to a specific member of the debtors section by the use of user ID & passwords ■ 3.2 All masterfile amendments should be automatically logged by the computer on **sequenced** logs and there should be **no write access** to the logs ■ 3.3 To enhance the accuracy & completeness of the keying in of masterfile amendments and to **detect invalid conditions**, screen aids & programme checks will be implemented ***Screen aids and related features*** • minimum keying in of information. For example when amending existing debtors records, the user will only key in the debtors account number to bring up all the details of the debtor ■ • screen formatting, screen looks like MAF, screen dialogue

▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪	▪ • new debtors account number automatically generated by the system ▪ ***Programme checks*** e.g. • verification / matching checks to validate a debtor account number against the debtors masterfile (invalid account number, no amendment) • alpha numeric checks • range and / or limit / data approval checks on terms and credit limit field, e.g. credit limit must be between R 5000 and R 75000 (range) or cannot exceed R 75000 (limit), and terms can only be 30 days or 60 days (data approval) • field size check & mandatory / missing data checks, e.g. credit limit & terms must be entered • sequence check on MAFs entered • dependency checks e.g. the credit limit granted may depend upon the credit terms granted, e.g. a debtor granted payment terms of 90 days may only be granted credit up to a limit of R 2000
4. Review masterfile amendments to ensure they occurred, were authorised & were accurately and completely processed	4.1 The logs should be reviewed regularly by a senior staff member e.g. financial manager • the sequence of the logs should be checked (for any missing logs) 4.2 Each logged amendment should be checked to confirm that it is supported by a properly authorised MAF and 4.3 That the detail, e.g. debtor account number, amounts, etc. are correct 4.4 The MAFs themselves should be sequence checked against the log to confirm that all MAFs were entered

Can you recall that input of data can be either: **batch input** or **on-line input**?
These two methods can be described as follows:

Batch input

Batch input depend on two steps: **data preparation** and the **keystroke entry of data**.

Data preparation is an off-line process in batch entry systems by means of which:

- Data is manually captured, which includes initiating, recommending, authorising and preparing documentation for the transaction.
- Data is collected into batches for input into the computer.

The **keystroke entry of data** is a process where data is keyed in, converted and encoded in machine readable form and held in a transaction file on the computer system. During this process a series of programmed application controls are applied to make certain that the data is reliable and correct before it is processed.

On-line input

Transaction data is entered, via a keyboard, immediately as each transaction occurs. With online input, batch data preparation is not required and the control approach required differs from the approach required for batch input. The on-line input approach involves immediate data validity testing and batch controls that operate after (instead of before) input. This approach relies heavily on general controls.

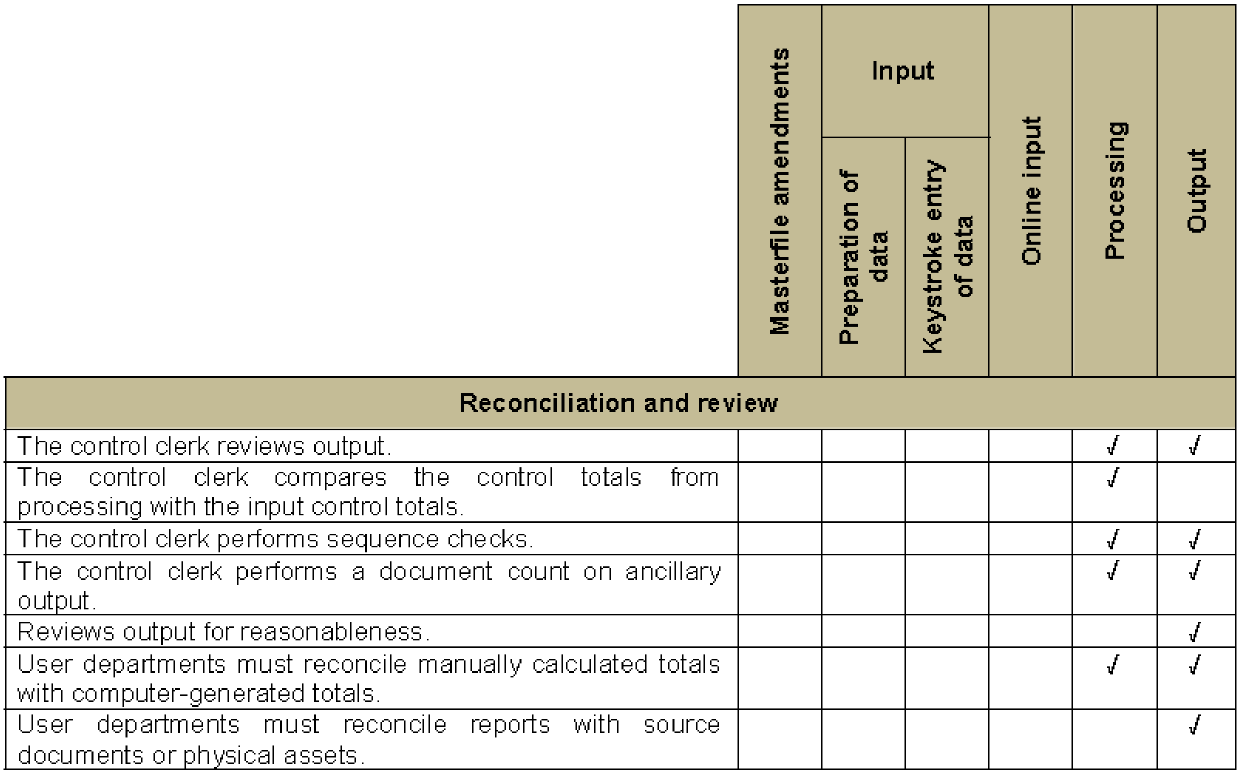
Table 1

Controls applicable to masterfile amendments, input, processing and output

	Masterfile amendments	Input		Online input	Processing	Output
		Preparation of data	Keystroke entry of data			
Authorisation						
Signatures of supervisory personnel, or the electronic equivalent, must appear on source documents and batch forms.	✓	✓				
Access to the input module of an application must be restricted.	✓		✓	✓		
Access to source documents						
Unused source documents must be kept by a person who is independent of the application.	✓	✓				
Source documents must be prenumbered and a register must be kept of receipts and issues of blank source documents.	✓	✓				
Source document design						
All information that remains unchanged must be preprinted and copies of the same document must be in different colours.	✓	✓				
If a limited number of answers are applicable, the document must be designed in such a way that the user only marks off the applicable answer.	✓	✓				
The title of the document must indicate the purpose of the document.	✓	✓				
Notes and instructions must appear on the document to make it easier to complete.	✓	✓				
Boxes must be used to prevent field size errors.	✓	✓				
The fields to be filled in must appear in the sequence in which data is entered, as determined by the program.	✓	✓				
Source documents must be prenumbered to make sequence checks possible.	✓	✓				
Management review						
An independent person must review another person's work.	✓	✓				
Audit trails of transactions, override logs and exception reports must be inspected by senior personnel.	✓		✓	✓	✓	
Batch controls						
Source documents must be grouped into batch sizes and control totals must be calculated. The following are different types of control totals that can be calculated: financial totals, hash totals and record counts.		✓				

	Masterfile amendments	Input		Online input	Processing	Output
		Preparation of data	Keystroke entry of data			
A batch control sheet must be prepared and attached to a batch.		✓				
A batch register must be used to document the physical progress of a batch.	✓	✓	✓	✓	✓	✓
Details of the batch must be captured on a computer to create a batch header label.	✓	✓	✓	✓	✓	✓
Records in the batch must be captured on computer and subjected to programmed validity controls.	✓	✓	✓	✓	✓	✓
Once all the records in the batch have been keyed in, the computer must compute its own control total on the basis of the information that has been captured. The computer then compares this total with the manually calculated control total calculated by the user before input into the computer. The batch header label is then automatically updated with the control total calculated by the computer.	✓	✓	✓	✓	✓	✓
If the control totals agree, the batch is accepted for processing. If they do not agree, the batch is rejected and returned for correction.	✓	✓	✓	✓	✓	✓
The computer-calculated control totals must be updated on the batch header label. The batches can then go through the rest of the process.	✓	✓	✓	✓	✓	✓
Access controls						
Access to a particular application must be restricted.	✓		✓	✓		
Physical access to computers that contain sensitive applications must be restricted.	✓		✓	✓		
Access must be restricted by means of user profiles or access tables at both the systems level and the application level.	✓		✓	✓		
Computer time-out facilities and automatic time-out should come into operation as soon as unauthorised access is obtained.	✓		✓	✓		
User ID and computer logging of all activities must be introduced.	✓		✓	✓		
Screen aids						
Keying in of the minimum information.	✓		✓	✓		
Fields on the computer screen must appear in the same sequence as in the source document.	✓		✓			
Screen format: the computer screen must be formatted in the same way as the hard copy of the source document.	✓		✓			
Screen dialogue and prompts.	✓		✓	✓		
Mandatory fields.	✓		✓	✓		
Verbal confirmation of data.				✓		

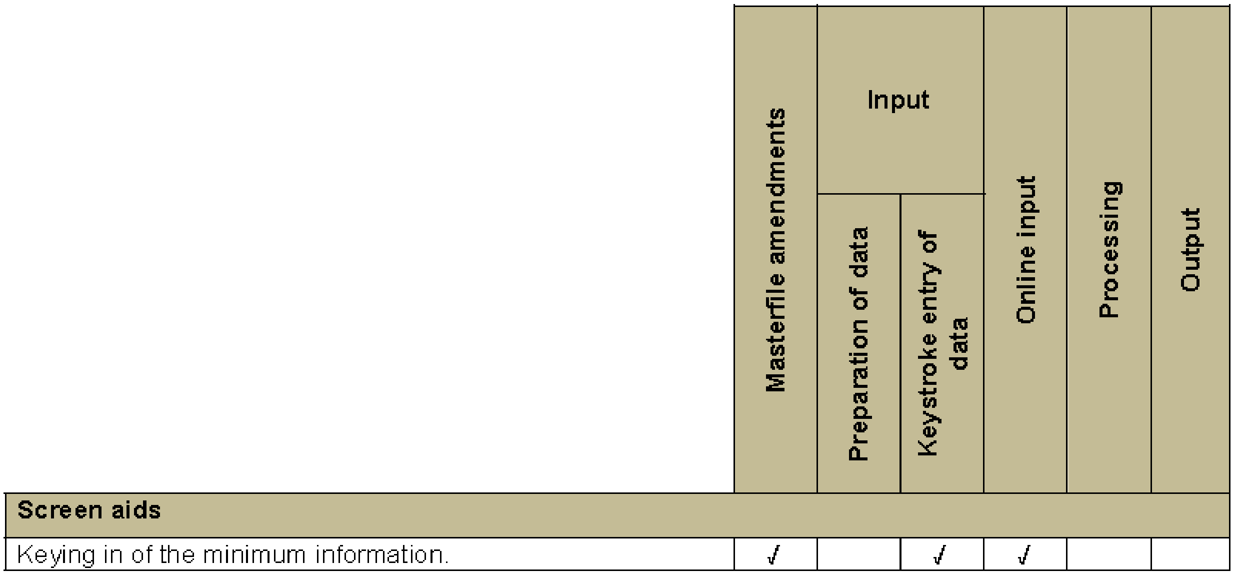
	Masterfile amendments	Input		Online input	Processing	Output
		Preparation of data	Keystroke entry of data			
Shading of fields	✓		✓	✓		
Programme checks						
Alpha-numeric check	✓		✓	✓		
Range test	✓		✓	✓		
Limit check	✓		✓	✓		
Check digit			✓	✓		
Size check	✓		✓	✓		
Missing data check/mandatory field check	✓		✓	✓		
Reasonableness check/consistency check	✓		✓	✓		
Sequence check	✓		✓	✓		
Verification check/validation check	✓		✓	✓		
Data approval check/authorisation check	✓		✓	✓		
Internal label check					✓	
Generation number check					✓	
Retention date check					✓	
Arithmetic accuracy check	✓		✓	✓		
Cross cast/accuracy check	✓		✓	✓		
Run-to-run totals					✓	
Matching check	✓		✓	✓		
Dependency check	✓		✓	✓		
Valid character and sign check	✓		✓	✓		
Logs and reports						
Audit trails	✓		✓	✓	✓	✓
Run-to-run balancing reports					✓	
Override reports	✓		✓	✓	✓	✓
Exception reports	✓		✓	✓	✓	✓
Before-and-after images					✓	
Activity reports	✓		✓	✓	✓	✓
Computer-generated transaction listing					✓	✓
Access/violation reports	✓		✓	✓	✓	✓
Output handling controls						
Clear report identification.						✓
A distribution matrix must be compiled.						✓
Output must be recorded in a dispatch register to control movement.						✓
The design of stationery must promote confidentiality.						✓
Confidential information for employees should not be e-mailed to their work PCs						✓
The print function for the printing of confidential information must be restricted to printers that are under the supervision of appropriate officials.						✓
All output which is not required must be shredded.						✓



	Masterfile amendments	Input		Online input	Processing	Output
		Preparation of data	Keystroke entry of data			
Reconciliation and review						
The control clerk reviews output.					√	√
The control clerk compares the control totals from processing with the input control totals.					√	
The control clerk performs sequence checks.					√	√
The control clerk performs a document count on ancillary output.					√	√
Reviews output for reasonableness.						√
User departments must reconcile manually calculated totals with computer-generated totals.					√	√
User departments must reconcile reports with source documents or physical assets.						√

Instruction for using table 2

Certain of the application controls are applicable to a combination of masterfile amendments, input, processing and output. For example, the screen aid that requires the minimum keying of information is applicable to masterfile amendments, the keystroke entry of data and online input. This is illustrated by the following extract from table 1:



	Masterfile amendments	Input		Online input	Processing	Output
		Preparation of data	Keystroke entry of data			
Screen aids						
Keying in of the minimum information.	√		√	√		

In table 2 we supply only one example that pertains to **either** masterfile amendments **or** the keystroke entry of data **or** online input. After the example, the relevant aspect is indicated in brackets. The following extract from table 2 serves as an example:

Control	**Explanation of control with reference to an example**
Keying in of the minimum information.	If a sales invoice is keyed in, the client's name and address will automatically appear as soon as the client number is keyed in. Because the name and address appear automatically, possible transcription errors are avoided. **(Keystroke entry of data)**

In table 2, after the example, the **control objective** achieved by the relevant application control is indicated in brackets. The following extract from table 2 serves as an example:

Control	**Explanation of control with reference to an example**
Keying in of the minimum information.	If a sales invoice is keyed in, the client's name and address will automatically appear as soon as the client number is keyed in. Because the name and address appear automatically, possible transcription errors are avoided. **(Keystroke entry of data – Accuracy)**

Table 2

Explanation of controls with reference to appropriate examples

Control	Explanation of control with reference to an example
Authorisation	
Signatures of supervisory personnel, or the electronic equivalent, must appear on source documents and batch forms.	Before Mr T can change the opening balance of a debtor's account, a written request must be signed by the head of the sales department. **(Masterfile amendments – Occurrence and authorisation)**
Access to the input module of an application must be restricted.	Mrs X is the only person who can change the opening balances of inventory items. Management must implement access tables to ensure that only Mrs X can gain access to the inventory masterfile. **(Masterfile amendments – Occurrence and authorisation)**
Access to source documents	
Unused source documents must be kept by a person who is independent of the application.	Unused sales invoices must be kept in the operational manager's safe. **(Preparation of data – Occurrence and authorisation)**
Source documents must be prenumbered and a register must be kept of receipts and issues of blank source documents.	Mr T orders 100 unused, preprinted sales invoices from the supplier. He asks the supplier to number the sales invoices from 678 to 778 and bind them in sales invoice books of ten each. Upon receipt Mr T records these ten books in a log. As the books are issued to sales consultants, the log is updated. **(Preparation of data – Occurrence and authorisation)**
Source document design	
All information that remains unchanged must be preprinted and copies of the same document must be in different colours.	The following information should be preprinted on a sales invoice: name of the sales agent, name of the purchaser, client code, description of the stock, quantity, total etc. Three copies of the sales invoice are required. Copy 1 is white and remains in the sales invoice book, copy 2 is pink and is given to the purchaser, and copy 3 is yellow and is sent to the inventory department. (**Data preparation – Accuracy)**
If a limited number of answers are applicable, the document must be designed in such a way that the user only marks off the applicable answer.	A company sells only 3 kinds of products. Instead of the sales consultant writing down the item sold, the sales invoice should be designed in such a way that it lists the 3 types of product. The sales consultant then merely marks off the item(s) sold. **(Data preparation – Accuracy)**
The title of the document must indicate the purpose of the document.	The sales document must clearly indicate the following in capitals: **SALES INVOICE**. **(Data preparation – Accuracy)**
Notes and instructions must appear on the document to make it easier to complete.	The following instructions should appear on the reverse of the sales invoice:

Control	**Explanation of control with reference to an example**
	• All fields of the sales invoice must be filled in. • If a code has not yet been assigned to the client, a code must first be obtained from the credit department before the other fields are filled in. **(Data preparation – Accuracy)**
Boxes must be used to prevent field size errors.	The following could appear on a sales invoice: **Purchaser's code** □□□□ The four boxes make it easier to complete the purchases code field. If the code had three or five figures, for example, it would immediately be apparent that a mistake had been made. **(Data preparation – Accuracy)**
The fields to be filled in must appear in the sequence in which data are entered, as determined by the program.	The computer program requires information to be entered on the sales module in the following sequence: 1. Name of purchaser 2. Purchaser's code 3. Date, etc It is important that the above fields should appear in the same sequence on the sales invoice. **Data preparation – Accuracy)**
Source documents must be prenumbered to make sequence checks possible.	As sales take place, the following prenumbered sales invoice is used in the sales book. At the end of the month an independent person ensures that there are no missing numbers in the sales invoices. If, say, sales invoice 67 is missing, the matter would be investigated. **(Data preparation – Completeness)**
Management review	
An independent person must review another person's work.	After the sales consultant has completed the sales invoice, it is reviewed by the head of the sales department. (**Data preparation – Occurrence and authorisation, accuracy, completeness)**
Audit trails of transactions, override logs and exception reports must be inspected by senior personnel.	Mr X may only change the opening balances of inventory items if the change involves less than five items. Changes involving more than five items must be made by Mr Y. Exception reports of all inventory item changes involving more than five items are kept up to date by the computer. They are inspected by a senior person to ensure that a masterfile amendment of this nature has been duly authorised and made by Mr Y. **(Masterfile amendments – Occurrence and authorisation, accuracy, completeness)**

<table>
<tr><th>Control</th><th>Explanation of control with reference to an example</th></tr>
<tr><th colspan="2">Batch controls</th></tr>
<tr><td>Source documents must be grouped into batch sizes and control totals must be calculated. The following are different types of control totals that can be calculated: financial totals, hash totals and record counts.</td><td>At the end of each week clock cards are collected and grouped into bundles of 15 clock cards each. The following types of control totals can be computed for a batch:

• Financial totals: The rand values of the amount to which each of the workers is entitled, as it appears on the 15 clock cards, is totalled.
• Cash totals: Arbitrarily chosen numerical fields on the clock cards are added, for example the employee numbers that appear on the clock cards.
• Record count: Count how many physical records there are in the batch – eg there are 15 clock cards in the batch, so the record count is 15.

Remember that these control totals serve no purpose unless the system computes them later and compares them with the original control totals. Control totals should therefore be compared and calculated before and after input, before and after processing and before and after output to ensure that the data are still accurate, complete, occurred and are authorised and that nothing has been added or erased.

<b>(Data preparation – Occurrence and authorisation, accuracy, completeness)</b></td></tr>
<tr><td>A batch control sheet must be prepared and attached to a batch.</td><td>There are 15 clock cards in the batch. A batch control sheet is attached to the front of each batch. The following information appears on the batch control sheet: the batch number (eg 234), the batch size (eg 15), what the batch consists of (eg clock cards), the fields where the control totals can be filled in before and after processing, and before and after output. The batch control sheet could also contain a space for the signature of the person dealing with the batch. The batch control sheet accompanies the batch throughout the input, processing and output processes. This is a control that monitors the progress of the batch during the process.

<b>(Data preparation – Accuracy, completeness)</b></td></tr>
<tr><td>A batch register must be used to document the physical progress of a batch.</td><td>The following is a visual representation of a batch register:

<table>
<tr><th>Batch no.</th><th>Details</th><th>Input</th><th>Processing</th><th>Output</th></tr>
<tr><td>1</td><td>15 clock cards</td><td>Mrs Z</td><td>Mr O</td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td><td></td></tr>
<tr><td>4</td><td></td><td></td><td></td><td></td></tr>
</table>

It is clear from the above representation that batch no. 1 is in the processing stage, with Mr O.

<b>(Processing – Occurrence and authorisation, accuracy and completeness)</b></td></tr>
</table>

Control	Explanation of control with reference to an example
Details of the batch must be captured on a computer to create a batch header label.	The batch details and initial control totals calculated before input are entered on the computer by keystroke entry. This is a machine-readable record containing the following, for example: 15 clock cards, control total before input: R567 989. **(Data preparation, keystroke entry – Occurrence and authorisation, accuracy and completeness)**
Records in the batch must be captured on computer and subjected to programmed validation controls.	As information is entered, the computer carries out preprogrammed checks. For example, the computer has been preprogrammed to ensure that wage workers may not clock more than 8 hours a day. If a clock card on which a worker has clocked more than 10 hours is entered, the computer displays an error message. This test is known as a limit test. Programmed validation controls are discussed in detail later on. **(Keystroke data entry – Occurrence and authorisation, accuracy)**
Once all the records in the batch have been keyed in, the computer must compute its own control total on the basis of the information that has been captured. The computer then compares this total with the manually calculated control total calculated by the user before input into the computer. The batch header label is then automatically updated with the control total calculated by the computer.	After input the computer automatically recalculates the control total, say as R567 989. The batch header label is then automatically updated. The control total that was keyed in on the batch header label before input is compared with the control total calculated by the computer after input. **(Keystroke data entry – Occurrence and authorisation, accuracy and completeness)**
If the control totals agree, the batch is accepted for processing. If they don't agree the batch is rejected and returned for correction.	If the manually calculated control total of R567 989 agrees with the computer-calculated control total after input, the user has the assurance that all the information is still accurate, valid and complete and that processing can proceed. **(Keystroke data entry – Occurrence and authorisation, accuracy and completeness)**
The computer-calculated control totals must be updated on the batch header label. The batches can then go through the rest of the process.	The computer-calculated control total of R567 989 is updated on the batch header label, after which the computer can calculate the control total throughout the process. That is, the computer recalculates the control total during input, processing and output to ensure that the control total of R567 989 remains unchanged. **(Processing and output – Occurrence and authorisation, accuracy and completeness)**
Access controls	
Access to a particular application must be restricted.	Mrs R and Mr J are the only members of staff who work with the wages and salary application. A control can therefore be introduced to ensure that this application can only be accessed from Mrs R and Mr J's computers. (**Masterfile amendments, keystroke data entry, online input and output – Occurrence and authorisation)**

Control	Explanation of control with reference to an example
Access to computers that contain sensitive applications must be restricted.	Mrs R and Mr J's offices, where their computers are housed, must be locked at all times, if they are not present. Nobody else (except security officers in emergencies) may possess a duplicate key. **(Masterfile amendments, keystroke data entry, online input and output – Occurrence and authorisation)**
Access must be restricted by means of user profiles or access tables at both the systems level and the application level.	Mrs R is responsible for all matters concerning wages in the wages and salaries application. Mr J is only concerned with salaries in the wages and salaries application. At systems level access to the system can be controlled by instituting user identities for Mrs R and Mr J. At application level, access to the wages and salaries application is restricted to Mrs R and Mr J. Access to all wage functions is further restricted to Mrs R and access to all salaries functions to Mr J. **(Masterfile amendments, keystroke data entry, online input and output – Occurrence and authorisation)**
Computer time-out facilities and automatic time-out should come into operation as soon as unauthorised access is obtained.	If Mrs R does not work on the payroll functions for 15 minutes, the computer will automatically shut down. She will only be able to gain access again by logging on and keying in her password. If the computer suspects that someone other than Mrs R is working on the payroll functions, the computer will automatically shut out further actions and no further actions will be permitted. **(Masterfile amendments, keystroke data entry, online input and output – Occurrence and authorisation)**
User ID and computer logging of all activities must be introduced.	The computer automatically logs the following information: the identities of all users who have accessed the payroll functions as well as all the activities carried out on the payroll functions by these users. This log must be inspected by senior management at the end of each week. If this log indicates that a user other than Mrs R has accessed the payroll functions, this must be followed up immediately since it could indicate fraud. **(Masterfile amendments, keystroke data entry, online input and output – Occurrence and authorisation)**
Screen aids	
Keying in of the minimum information.	If a sales invoice is keyed in, the client's name and address will automatically appear as soon as the client number is keyed in. Because the name and address appear automatically, possible transcription errors are avoided. **(Keystroke data entry - Accuracy)**
Fields on the computer screen must appear in the same sequence as in the source document.	The information on the sales invoice is given in the following sequence: debtor's name, debtor code, sales item(s), quantity sold etc. The computer screen must display the information in the same sequence in order to make keying in easier. **(Keystroke data entry - Accuracy)**

Screen format: the computer screen must be formatted in the same way as the hard copy of the source document.	The computer screen must look exactly the same as the sales invoice. For example, spaces must appear in exactly the same places – if the sales invoice allows 10 spaces for the client code, the computer screen must also show 10 spaces. **(Keystroke data entry - Accuracy)**
Screen dialogue and prompts.	An input clerk is requested by senior management to adjust a debtor's outstanding balance. The computer guides the input clerk through the input process. The cursor moves from one input field to the next to show the clerk where to key in the information. **(Masterfile amendments - Accuracy)**
Mandatory fields.	The sales document is entered and the clerk confirms complete input by pressing the "enter" key on the keyboard. However, the computer displays an error message, "Not all mandatory fields have been keyed in, please enter the client code". The computer will not allow the clerk to key in any other sales documents before the compulsory client code has been entered. **(Keystroke data entry – Accuracy, completeness)**
Verbal confirmation of data.	An enterprise receives all customer orders by telephone. After the orders have been taken, the input operator reads the details of the order back to the client to confirm that the correct information has been keyed in. **(Online input – Accuracy)**
Shading of fields.	A customer's account number and details are shaded and cannot be changed if "clicked on". **(Keystroke data entry – Accuracy)**
Programme checks	
Alpha-numeric check	Certain input fields may only consist of numbers and others only of alphabetical letters. Some fields may contain a combination of numerical and alphabetical characters. For example, if the number of hours on a clock card is entered on the computer as 3a instead of 31, the computer will display an error message, since that field may only contain numerical characters. **(Keystroke entry of data – Accuracy)**
Range test	The computer is programmed to display an error message if the field that is filled in falls outside predetermined minimum and maximum values. The quantity of items ordered per a sales order form may not be less than 1 and may not exceed 50 items. Therefore, if 51 items are keyed in, the computer will display an error message. In addition, if 0.5 items are keyed in, the computer will also display an error message. **(Keystroke data entry – Accuracy)**
Limit check	The limit of a total that may be entered is predetermined. For example, the number of hours worked per week as entered on the clock card must not be more than 40. Therefore, if 41 are keyed in, the computer will display an error message. **(Keystroke data entry – Accuracy)**

Control	Explanation of control with reference to an example
Check digit	The computer calculates a check digit on the basis of the logical relationship between the characters in a field. An extra check digit is attached to the end of the characters of a field. For example, an enterprise that sells spares allocates spares numbers to each type of product. An initial check digit is attached to the end of a spares number. When the spares number is input during a sales transaction, the computer recalculates the check digit and compares it with the check digit initially allocated to the spares number. If they differ, the computer displays an error message that could indicate that an error has been made during the entry of the spares number. **(Keystroke data entry – Accuracy)**
Size check	Certain input fields must contain a certain number of characters. If an employee number should consist of 8 characters, a field size check will be carried out to ensure that 7 or 9 characters are not keyed in. **(Keystroke data entry – Accuracy)**
Missing data check/Mandatory field check	This check detects blank fields. For example, it is a requirement that an employee number should be keyed into the appropriate field when clock cards are entered. If this field is not keyed in and the input clerk wants to continue processing the clock card, the computer will display an error message and request the clerk to fill in the blank field first. **(Keystroke data entry – Completeness)**
Reasonableness check/Consistency check	It is possible that the clock card of a half-day wage worker may pass the limit test if it shows 40 working hours for the week. (According to the limit test the number of working hours per week must be 40 or less.) However, the clock card would not pass the reasonableness check, because the computer would compare the number of working hours with the employee's status – for example a half-day wage worker may only work 20 or less hours per week. **(Keystroke data entry – Occurrence and authorisation, accuracy and completeness)**
Sequence check	Your enterprise employs 20 wage workers. Their clock card numbers are 1-20. If the clock cards are keyed in weekly but clock card 11 is not keyed in, the sequence test will detect the error. **(Keystroke data entry – Completeness)**
Verification check/Validation check	The computer saves a list of valid debtors numbers in a masterfile. If orders are placed telephonically and entered by the telephone operator, the following situation may arise: a telephonic order is only accepted if a client gives his debtor's number and it is accepted by the computer system. As soon as the debtor's number is keyed in, the computer compares it with a list of valid debtors numbers. If the computer finds that no such debtor's number exists, this could mean that the clerk has made an error with the input of the number or that the client has supplied an invalid debtor's number. **(Online input – Occurrence and authorisation, accuracy)**

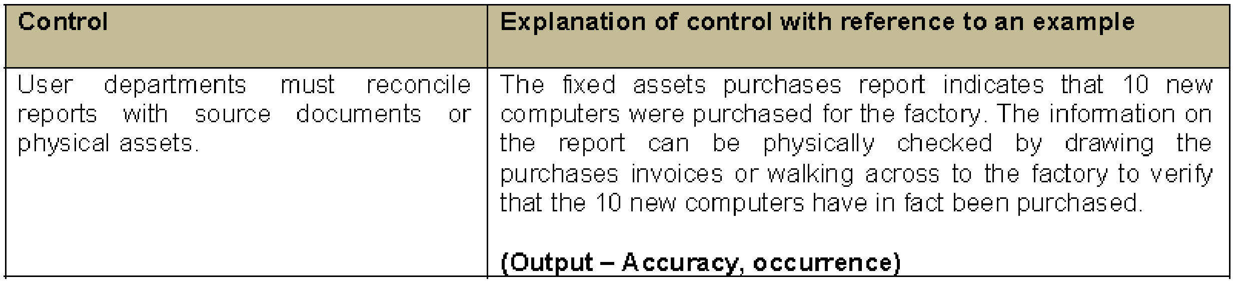
Control	Explanation of control with reference to an example
Data approval check/Authorisation check	The computer determines whether the transaction that has been entered is feasible, in other words whether it complies with management's policy and conditions. It could, for example, be management policy that a person may not buy on credit if his account is more than 120 days in arrears. If a sales invoice has been keyed in, the computer will check whether the client's account is more than 120 days in arrears before approving the transaction. **(Keystroke data entry – Occurrence and authorisation, accuracy)**
Internal label check	An internal label of a salary file will contain the name and date of the file. If the inventory masterfile has to be updated with the monthly sales transactions but the salary file is accidentally loaded for this process, the computer will read the salary file's internal label and immediately indicate that the wrong file is being used to update the inventory masterfile. **(Processing – Occurrence and authorisation)**
Generation number check	This test ensures that the correct version of the file has been loaded. In other words this test ensures that the latest file has been loaded and not an old version. The salaries masterfile which has to display the total income for each employee up to the present for the 2012 financial year is updated monthly with the latest salary file. Three versions of the salaries masterfile are kept up to date on a grandfather, father and son basis. If an older version of the salaries masterfile (eg the father file) is used to create the latest masterfile by updating it with the salaries file, the computer will immediately detect that the wrong generation of file (eg the father file instead of the son file) has been used. **(Processing – Occurrence and authorisation)**
Retention date check	This is a test that a computer performs on a file to determine whether the file has already expired. For example, if the inventory masterfile has to be updated with the monthly sales file, the computer will check whether the file covers the correct sales period that must be used during processing. If the sales file for the period 1 January to 31 January **2012** should be used, the computer will immediately detect the error if a sales file for the period 1 January to 31 January **2011** is used instead. **(Processing – Occurrence and authorisation)**
Arithmetic accuracy check	When clock cards are captured the hourly tariff is multiplied by the number of hours worked, for example, R20 per hour x 6 hours = R120. The multiplication is now reversed and the answers compared to ensure that the answer has been correctly calculated, in other words: 120 / 6 hours = 20. **(Keystroke data entry – Accuracy)**

<table>
<tr><th>Control</th><th>Explanation of control with reference to an example</th></tr>
<tr><td>Cross cast/Accuracy test</td><td>Study the following representation:
<table>
<tr><th>Worker</th><th>Gross salary</th><th>Less medical</th><th>Less tax</th><th>Net salary</th></tr>
<tr><td><b>X</b></td><td>100k</td><td>10k</td><td>20k</td><td>70k</td></tr>
<tr><td><b>Y</b></td><td>90k</td><td>10k</td><td>10k</td><td>70k</td></tr>
<tr><td><b>Z</b></td><td>80k</td><td>10k</td><td>5k</td><td>65k</td></tr>
<tr><td><b>Total</b></td><td></td><td></td><td></td><td><b>205k</b></td></tr>
</table>
To test the result of 205, the computer will add the totals of the columns and use these totals to recalculate the total of the net salaries (see the schematic representation given below).
<table>
<tr><th>Worker</th><th>Gross salary</th><th>Less medical</th><th>Less tax</th><th>Net salary</th></tr>
<tr><td><b>X</b></td><td>100k</td><td>10k</td><td>20k</td><td>70k</td></tr>
<tr><td><b>Y</b></td><td>90k</td><td>10k</td><td>10k</td><td>70k</td></tr>
<tr><td><b>Z</b></td><td>80k</td><td>10k</td><td>5k</td><td>65k</td></tr>
<tr><td><b>Total</b></td><td><b>270k</b></td><td><b>30k</b></td><td><b>35k</b></td><td><b>205k</b></td></tr>
</table>
<b>(Keystroke data entry – Accuracy, completeness, occurrence)</b></td></tr>
<tr><td>Run-to-run totals</td><td>A final debtors balance (total of the balances of the individual debtors accounts) after processing is tested as follows: the total of the opening balances of individual debtors accounts plus the total of the sales transactions, minus the total payments received from the debtors is calculated. The final debtors balance calculated in this way is compared with the balance calculated after processing the individual debtors accounts.
The following test would be carried out by the computer, for example, to determine whether the processing result is correct:
<table>
<tr><td>Opening balance of individual debtors accounts</td><td>R180k</td></tr>
<tr><td><i>Plus</i>: Total of sales transactions</td><td>R180k</td></tr>
<tr><td><i>Minus</i>: Total of debtors payments</td><td>R50k</td></tr>
<tr><td><b>Total:</b></td><td><b>R310k</b></td></tr>
</table>
The result of the above calculation of R310k is compared with the closing balances of the individual debtors accounts, namely:
<table>
<tr><td>Debtor A:</td><td>R130k</td></tr>
<tr><td>Debtor B:</td><td>R100k</td></tr>
<tr><td>Debtor C:</td><td>R80k</td></tr>
<tr><td><b>Total:</b></td><td><b>R310k</b></td></tr>
</table>
<b>(Processing – Accuracy, completeness, occurrence)</b></td></tr>
<tr><td>Matching check</td><td>The computer matches the details of an invoice received from a supplier to the corresponding goods received note (GRN) held in a suspense file on the system.
<b>(Keystroke data entry – Occurrence and authorisation, accuracy)</b></td></tr>
</table>

Control	Explanation of control with reference to an example
Dependency check	XYZ (Pty) Ltd allocates a credit limit to a debtor based on its assigned status. An A rating debtor can be allocated a credit limit of R100 000 and a B rated debtor a credit limit of R50 000. Mr V captured a credit limit of R100 000 for a B rated debtor. The system performs a dependency check and displays a fault message. **(Keystroke data entry – Occurrence and authorisation)**
Valid character and sign check	An employee number captured onto the system cannot contain a minus (-) sign. **(Keystroke data entry – Accuracy)**
Logs and reports	
Audit trails	The computer provides a table with interest rates used for levying interest on arrear accounts. These tables can be studied by the senior manager to determine whether the correct interest rates have been applied. **(Processing – Occurrence and authorisation, accuracy, completeness)**
Run-to-run balancing reports	These are computer-generated reports that provide evidence that the opening balances of debtors have been updated with sales and back payment transactions to reflect the correct debtors closing balances. **(Processing – Accuracy, completeness)**
Override reports	This is a report listing all controls that have not been complied with and that therefore blocked the processing of transactions although the transactions were eventually authorised and accepted by management. For example, an employee on the lowest wage scale may not receive a wage of more than R5 000 per week. A clock card is processed and an error message displayed because an employee has received a wage of R6 000. The senior manager investigates the incident and ultimately approves it because the worker worked overtime. This action by the senior manager appears on a report and is checked by an independent senior member of staff. **(Processing – Occurrence and authorisation)**
Exception reports	An exception report is a report listing all transactions that fell outside the parameters of the programmed computer controls but that were eventually processed. For example, all the clock cards that show more than 40 hours per week and therefore fall outside the predetermined limit of a maximum of 40 hours per week will appear on an exception report. **(Processing – Occurrence and authorisation, accuracy)**
Before-and-after images	A record is kept of database information before and after updating, for example a database of debtors closing balances before and after updating. If it is established that errors occurred during the updating of the debtors database, the database as it was before the updating can be used again. **(Processing – Occurrence and authorisation, accuracy, completeness)**

Control	Explanation of control with reference to an example
Activity reports	This is a report showing all the activities on an application, for example the payroll application. It indicates who used the application, and when and for how long they used it. For example, if Mrs V always amended the masterfile on the payroll application around midnight, and usually over weekends, this may be a sign that unauthorised changes were made. **(Masterfile amendments – Occurrence and authorisation)**
Computer-generated transaction listing	If a computer automatically updates the inventory system after the updating of all sales transactions, the computer will automatically place new orders for inventory that has reached a specific predetermined minimum quantity. A report showing these automatically generated transactions can be requested for review. **(Processing – Occurrence and authorisation, accuracy, completeness)**
Access/violation reports	This is a report showing all unauthorised users that, for example, accessed the company's bank account and performed electronic fund transfers. **(Processing – Occurrence and authorisation)**
Output handling controls	
Clear report identification.	The following information must appear on the front cover of the report on the 10 top selling items: TOP 10 BEST SELLERS FOR THE PERIOD: 1 APRIL 2012-12 APRIL 2012 REPORT CREATED ON 12 APRIL 2012 AT14:00 Each page of the report must be numbered in sequence, to prevent the unauthorised removal of pages. **(Output – Correct and confidential distribution, completeness)**
A distribution matrix must be compiled.	The output clerk must draw up a list of all the types of reports that will be printed by a computer and the people who are authorised to receive these reports. **(Output – Correct and confidential distribution)**
Output must be recorded in a dispatch register to control movement.	A dispatch register must be compiled. As soon as the output clerk hands the report on the top 10 best sellers to Mr B, the description of the report must be recorded in the register, after which Mr B must sign the register as acknowledgement of receipt. **(Output – Correct and confidential distribution)**
The design of stationery must promote confidentiality.	The salary slips printed must be of the "sealed envelope" type. **(Output – Correct and confidential distribution)**

Control	Explanation of control with reference to an example
Confidential information for employees should not be e-mailed to their work PCs	If an employee requires that a soft copy of his salary slip should be e-mailed to him, this e-mail should only be sent to his personal PC. **(Output – Correct and confidential distribution)**
The print function for the printing of confidential information must be restricted to printers that are under the supervision of appropriate officials.	Salary slips may only be printed on the printer in the office of the Head of Human Resource Management. **(Output – Correct and confidential distribution)**
All output which is not required must be shredded.	If a second copy of salary slips is printed with carbon paper but not used, it must be destroyed to ensure that it is not examined or used by unauthorised users. **(Output – Correct and confidential distribution)**
Reconciliation and review	
The control clerk reviews output and processing activity reports.	A list of output that has been printed must be reviewed by the control clerk to ensure that all output requested has been printed. **(Output – Accuracy)**
The control clerk compares the control totals from processing with the input control totals.	The financial control total calculated during the input of the clock cards is R50 989. After processing the financial control total is calculated again and compared with the original control total of R50 989. **(Processing – Accuracy, completeness, occurrence)**
The control clerk performs sequence checks.	The control clerk checks the numerical sequence of the clock cards and ensures that clock cards 1-20 for the 20 wage workers employed have been processed. **(Processing – Completeness)**
The control clerk performs a document count on ancillary output.	Cheques are issued for the payment of creditors. If 30 creditor payments are processed, the control clerk must ensure that 30 cheques have been printed. **(Output – Completeness, occurrence)**
The user departments review output for reasonableness.	Salary payments are processed and the output is shown on the computer screen before the salary slips are printed. The human resource manager studies the information on the computer screen and notes that 20% of the salaries that are being paid out are less than R10. This is unreasonable and requires further investigation. **(Output – Accuracy, completeness)**
User departments must reconcile manually calculated totals with computer-generated totals.	The foreman calculates that the wage workers have collectively worked 6 000 hours. These 6 000 hours must be reconciled with the total number of hours worked and shown on the computer-generated wage report. **(Output – Accuracy, completeness, occurrence)**



Control	**Explanation of control with reference to an example**
User departments must reconcile reports with source documents or physical assets.	The fixed assets purchases report indicates that 10 new computers were purchased for the factory. The information on the report can be physically checked by drawing the purchases invoices or walking across to the factory to verify that the 10 new computers have in fact been purchased. **(Output – Accuracy, occurrence)**

Methods of obtaining & documenting an understanding of internal control systems

REMEMBER: An understanding of a client's internal control system 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.

NB: Components of internal control

1. The control environment
2. The entity's risk assessment process
3. The information system
4. Control activities
5. Monitoring of controls

1. Component: the control environment

The control environment sets the tone of the organization & influences the control consciousness of its staff. The directors and managers should, by their actions and behavior, promote an environment in which adherence to controls is regarded as very important. If managers set a bad example, ignoring controls & generally projecting a "slack" attitude, employees will soon adopt the same attitude. For example, a creditors clerk whose function it is to reconcile the creditors ledger accounts to the creditors statements, and then take the reconciliation to the financial accountant to be checked before payment is made, will soon not bother to reconcile properly, if at all, if she knows that the financial accountant does not check the reconciliation before authorizing the payment.

A good control environment will be characterized by:

1.1 communication and enforcement of integrity and ethical values throughout the organization;

▪

1.2 a commitment by management to competent performance throughout the organization;

▪

1.3 a positive influence generated by those charged with governance of the entity, e.g. non-executive directors, the chairperson (i.e. do these individuals display integrity & ethical commitment, are they independent, and are their actions and decisions appropriate?);

▪

1.4 a management philosophy and operating style which encompasses leadership, sound judgment, ethical behavior, etc;

▪

1.5 an organizational structure which provides a clear framework within which proper planning, execution, control and review can take place;

▪

1.6 policies, procedures & an organizational structure which clearly define authority, responsibility and reporting relationships throughout the entity;

▪

1.7 sound human resource policies and practices which result in the employment of competent ethical staff, provide training and development as well as fair compensation and benefits, promotion opportunities, etc

▪

Gathering of evidence relating to the control environment can be achieved by **observation** of management and employees "in action", including how they interact, **inquiry** of management and employees, e.g. union officials, and **inspection** of documents, e.g. codes of conduct, organograms, staff communications, records of dismissals, etc.

Generally a strong control environment will be a positive factor when the auditor assesses the risk of material misstatement. For example, the risk of fraud may be significantly reduced. A poor control environment, or elements of the control environment which are poor, will have the opposite effect, e.g. the company may have excellent human resource policies, but may lack leadership & organizational skills. Employees may be competent but management may have a "slack" attitude towards controls.

2. Component: the entity's risk assessment process

This is the process which the company has in place for, inter alia,

- ★ identifying business risks relevant to financial reporting objectives;
- ★ estimating the significance of each risk;
- ★ assessing the likelihood of its occurrence;
- ★ responding to the risk

This process of assessment of risk may be formal or informal. Larger organizations are more likely to have a formal plan, e.g. specific committees who hold regular meetings, the appointment of a Chief Risk Officer (CRO) and / or a Compliance Officer, but generally risk assessment is part of "managing". In doing their jobs, managers will identify and respond to risk.

Information about the client's risk assessment process will be gathered mainly by **inquiry**, e.g. Risk Officer, Compliance Officer, Chief Executive Officer, and **inspection** of documentation where it is available, e.g. minutes of designated committee meetings, inter-office memo's, on rectifying problems (responding to risk). An effective risk assessment process is advantageous for the auditor because the results produced by the in-house process provide the auditor with a platform to work from in assessing risk.

3. Component: the information system

The auditor is required to obtain an understanding of the information system relevant to financial reporting and communication. The accounting system is part of the information system. The auditor must obtain a thorough understanding of:

- ★ the classes of transactions in the client's operations that are significant to the financial statements, e.g. sales, wages

▪

★ the procedures within both IT and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements

▪

★ the related accounting records, supporting information and specific accounts in the financial statements in respect of initiating, recording, processing and reporting transactions

▪

★ how the information system captures events and conditions, other than transactions that are significant to the financial statements, e.g. contingent liabilities

▪

★ the financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures

▪

★ controls over the passing of non-standard journal entries used to record non-recurring, unusual transactions or adjustments

▪

★ the manner in which financial information is conveyed to management, the Board, the audit committee and external bodies, e.g. the JSE in the case of a listed company

▪

The chart below provides a breakdown of matters which the auditor might consider when obtaining information about a **computerized** information system.

Factor	Matters to consider
Computerised applications	▪ ★ which applications are computerised, e.g. - payroll – not computerized - acquisitions and payments – computerized ★ computer environment - micro, network, centralized - use of bureau ★ the application software - purchased or in-house software - key processing functions - nature and scope of inputs - output produced - important masterfiles and tables - interface between applications - new or established
Hardware	▪ ★ makes and capacities of CPU's, drives, printers, servers, terminals ★ physical location (branches, factory, etc)
Software	▪ ★ details of all software which is used for managing the functions of the hardware and data - operating systems

	- database management systems - utilities - access control software - programme change control software
Organisation and control	★ general and application controls ★ communication and reporting lines ★ IT personnel & their job descriptions ★ steering committee details ★ internal audit involvement in IT
Complexities of the system	★ the presence of: - networks (LANS, WANS) - electronic data interchange (EDI) - electronic funds transfer (EFT) - real time systems - the Internet - high levels of system integration - complex databases, communication networks
The level of dependence (of the client on its normal system)	★ degree of disruption which would occur if the system was not functioning for a lengthy period ★ the dependence of a particular functional area on timely, accurate computing, e.g. wages in a large labour intensive industry

The auditor should be mindful that computerised (IT) systems pose specific risks to an entity's internal control. These risks include the following:

1. A computer will process what is input & will do so in a manner in which it is programmed. If for example, there is an error in programming, that error will be repeated every time the relevant transaction is processed, e.g. a programming error results in the VAT on sales being calculated on the selling price plus VAT e.g. 14% of 114%. If 5000 invoices are processed the computer will make the mistake 5000 times.

▪

2. Unauthorised access to data can result in instant and huge destruction or contamination of data e.g. deletion of the debtors masterfile.

   ▪

3. IT personnel gaining access privileges they should not have, resulting in a breakdown of segregation of duties e.g. a systems analyst gains access to the salaries masterfile and alters his salary.

   ▪

4. Unauthorised changes to data in masterfiles, systems or programmes.

   ▪

5. Processing of fraudulent transactions instantaneously, e.g. unauthorized funds transfer which almost instantaneously moves money out of the company's bank account.

   ▪

6. Potential denial of access to electronic data e.g. can't get into the database because of system failure.

▪

The auditor should also be mindful that the information system as a whole, or elements of it, can be placed at risk, by for example:

★ **New employees** who have a different understanding of, or attitude to internal control, e.g. a newly appointed IT manager has a less strict attitude to access controls than his predecessor;

▪

★ **Rapid growth** in the company which places severe strain on the controls, e.g. a significant increase in the demand for the company's products has resulted in the company letting its creditworthiness checks lapse (so as not to lose sales) due to a lack of time and staff to carry out the checks. Automated (programmed) controls relating to creditworthiness may be overridden permanently or disabled;

▪

★ **New technology** which can lead to disruption of internal controls – introducing a network system may result in data being lost or corrupted;

▪

★ **Introducing new business models** which may result in the existing internal controls being rendered inadequate, e.g. introducing sales over the Internet to a long established (physical) retail business may introduce problems in controls over banking, receipt and dispatch of goods, etc.;

▪

★ **Corporate restructuring** which may result in staff reductions, new lines of authority etc., thereby jeopardizing for example, division of duties and authorisation controls

▪

Details of the information system (including the accounting system) can be gathered by:

1. **Inspection** (or creation) of flowcharts of the system;
2. **Observation** of the system in action, e.g. what happens when goods are delivered by a supplier;
3. **Inquiry** of client staff and the completion of internal control questionnaires;
4. **Discussions** with prior year audit staff, management and possibly outsiders, e.g. application software suppliers;
5. **Discussions** with internal audit staff and **review** of internal audit workpapers;
6. **Tracing** transactions through the information system, sometimes called "walk through" tests

4. **Component: control activities**

Control activities are the policies and procedures that are implemented to ensure that management's objectives are carried out.

Control activities include things such as:

★ authorisation of transactions (which is a form of isolating responsibility);

▪

★ segregation of duties .g. separating custody of inventory from keeping of inventory;

▪

★ physical control over assets, e.g. restricting access to the warehouse;

▪

★ comparison and reconciliation, e.g. reconciling the bank account monthly;

▪

★ access controls, e.g. access tables, user profiles, IDs and passwords in a computerised environment;

▪

★ custody controls over blank / unused documents, e.g. cheque books, order books;

▪

★ good document design (to achieve accuracy and completeness of information);

▪

★ sound general and application controls in IT systems

Information about control activities will usually be gathered in the same way as information about the information system as a whole is gathered, e.g. **inspection** of control procedures, manuals, **observation** of controls in action, **inquiry** of employees as to the procedures they carry out and the completion of internal control questionnaires.

5. **Component: monitoring of controls**

Monitoring of the system tells management how well the internal control process is doing over time. Management (and the board) wishes to know if controls are operating as intended and monitoring assists in providing this information. Monitoring as a component of the internal control process looks at **all of the components of the process** not only at the control activity component.

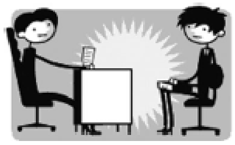
In larger companies, internal audit usually contribute to the effective monitoring of control activities, and the external auditor will frequently rely on work carried out by the internal auditor. Information from outside the company can also provide meaningful insight into whether the "system is working", e.g. monitoring complaints from customers will often give a good indication of aspects of the business which are not functioning as required.

Information about monitoring can be obtained by the auditor by **inquiry** of management and staff working with internal audit and **inspecting** documentation relating to a monitoring process or performance reviews.

The methods of obtaining information and knowledge comprise the following:

★ Walk-through tests of the system
★ Enquiries and discussions
★ Inspection of documentation
★ Observation of internal controls and processes
★ Internal control questionnaires

The following table describes the various methods use dto form an understanding of the components of internal control. Each method is explained with reference to an example.

Methods of obtaining an understanding of the various components of internal control	Description of method	Example
System walk-through tests	This is the process where an auditor selects a number of documents by which a certain transaction type is initiated & then follows the trail through the entire accounting process	The auditor chooses a purchase order for ordering stock & determines by means of a walk-through test whether it is made out in triplicate & that the first copy is sent to the creditor, the second to the accounts department & the third to the warehouse. The auditor does the same for all the transaction classes
Enquiries and discussions 	Meetings can be scheduled with management & the staff so that they can give the auditor information on the internal controls in the various transaction cycles. Information on the system can also be obtained by holding discussions with the previous year's audit personnel, third parties and the internal auditors	The scheduling of a meeting with the managing director to discuss the risk assessment process
Inspection of documentation	The auditor could study various documents in order to obtain an understanding of the internal controls present in the various transaction cysles	The study of systems flowcharts (prepared by the client), systems descriptions (prepared by the client), operating procedure manuals and the previous year's audit working papers
Observation of internal controls and processes	Internal controls and processes can be observed by the auditor	The auditor can determine through physical inspection what happens when goods are delivered by the supplier
Internal control questionnaires	Since internal control objectives and the way they are achieved are largely the same from one system to the	

	next, most auditors find that both efficiency & effectiveness are greatly increased by designing an internal control questionnaire (ICQ) to identify the expected internal controls. The ICQ is then used to document the internal control system. The ICQ is usually divided into transaction cycles covering the main transaction flows in a typical company. The ICQ can be classified on the basis of the internal control objectives that should be achieved by the client's internal controls at every stage of the transaction processing. The ICQ is also a convenient way of documenting the specific internal controls that the auditor wants to test for compliance. The questions in the ICQ are usually worded in such a way that only a "yes" or "no" answer is required to indicate the presence of absence of internal controls. An ICQ contributes to an auditor's understanding of the design and functioning of the internal control structure, but it does not contribute to an understanding of its effectiveness	

Activity:

Your firm has recently been appointed as the auditors of Echo Ltd, a company in the tourist industry. You are of the opinion that the use of internal control questionnaires would have many advantages for you as an auditor and that a questionnaire could be quickly compiled at the beginning of the audit.

Compile an internal control questionnaire that will enable you to evaluate Echo Ltd's internal control over their investments.

Feedback:

Internal control questionnaire:

Question	Yes	No	Comments
1. Are all the investment documents under the control of a custodian			
2. Are investment documents kept in a safe or in a safe-deposit box at the bank?			
3. Is the presence of more than one person required before the safe or safe-deposit box is opened?			
4. Are investment documents periodically inspected & reconciled with the accounting records?			
5. Does the securities custodian also have access to the accounting records?			
6. Are registered securities held in the name of Echo Ltd?			
7. If registered securities are not held in the name of the auditee, are they properly endorsed in blank, or in the name of an authorized agent or in the name of a nominee, or is a power of attorney attached?			
8. Are securities held as collateral or securities held for safekeeping for other parties properly segregated, both in the records and physically?			
9. Does the accounting department maintain an independent record of each investment security?			
10. Is all investment income properly accounted for?			
11. Are purchases and sales of investments properly authorized?			
12. Do the minutes of the board of directors authorize the acquisition of the securities of other companies?			

Activity:

Your firm has recently been appointed as the auditors of Local Architects (Pty) Ltd. The company uses information technology systems for their financial reporting and for operating purposes. They contacted you to discuss the specific risks that information technology involves for their internal control. You are of the opinion that the use of an internal control questionnaire enables you to obtain an understanding of the design and operation of the company's internal controls.

Draw up an internal control questionnaire that will enable you to obtain an understanding of the design and operation of Local Architects (Pty) Ltd's internal controls over unclaimed wages.

Feedback:

Internal control questionnaire:

Question	Yes	No	Comments
1. Do the paymaster & the foreman record the particulars of unclaimed wages in an unclaimed wages register?			
2. Does the paymaster keep the unclaimed wage envelopes & wages, and are they stored in a locked area?			
3. Do employees identify themselves to the paymaster when they collect unclaimed wages?			
4. When they collect unclaimed wages, do employees acknowledge receipt of their wage envelopes by signing the unclaimed wages register?			
5. Are periodical independent reconciliations between the unclaimed wage envelopes on hand and the unclaimed wages register carried out?			
6. Is the unclaimed wages register inspected for any unusual events?			
7. Are any wages that remain unclaimed after two weeks banked?			
8. Is a copy of the deposit slip with cross-references to the relevant entries attached to the register?			

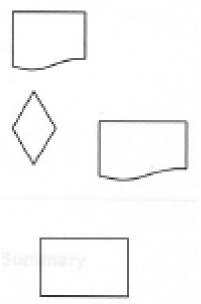
Methods of documenting the understanding of an internal control system that has been obtained

It is essential that an auditor record his understanding and knowledge of an entity's internal control system in audit working papers. There are several methods that the auditor could use to document the internal control processes of an entity. These methods include:

- ★ **Systems descriptions**

★ **Representation of systems and programs on flowcharts**

These methods are described below:

Methods of documenting the understanding of an internal control system obtained by the auditor	**Description**
A description of the system 	A description consists of the auditor's written comments on an auditee's internal control structure. These comments can be used to supplement other forms of documentation, because they are a summary of the auditor's general understanding of the internal control structure, individual elements of the internal control structure or other specific internal controls that are related to a specific control objective. For an audit of a small business, a description could serve as the onlhy documentation of the auditor's understanding of the internal control structure. In this case the description would indicate the sources of the knowledge that was obtained, and identify aspects of the internal control structure that are of importance for audit planning.
Flowcharts 	Systems and program flowcharts are used by auditors to represent the flow of information through the accounting system in visual terms. Systems flowcharts represent the broad flow of documents and data graphically, and program flowcharts illustrate the processing logic of computer programs in detail. There are numerous conventions for the preparation and use of systems and program flowcharts. These conventions cover aspects such as the flow of information and standardised symbols. Over the years audit firms have developed a variety of specialised techniques for compiling flowcharts. Flowcharts facilitate the overview and documentation of internal control systems. To understand or prepare a flowchart, an auditor must know the meaning of the specialised symbols that are used. Internal control flowcharts are usually prepared for accounting sub-systems such as cash receipts, wages, etc. If a system is too comprehensive, flowcharts can be compiled for a single class of transactions. Internal control flowcharts are usually divided into vertical columns, where each column represents a separate functional department (or an individual employee) responsible for the internal control activities for the processing of the relevant transactions. Flowcharts are usually arranged in such a way that processing begins either in the top right-hand

	corner or in the tope left-hand corner. Arrows and flow lines indicate the sequence of processing. The location and arrangement of files and multicopy documents in the department are shown by means of symbols. Important internal checkpoints can be identified and described by means of brief narrative descriptions.

The design of internal control systems

Basic functions for any revenue and receipts cycle:

(Insert photocopied pages into this section)

Framework that can be used in designing an internal control system for manual systems

1. Divide the system into **phases on the basis of the flow of information**:

- Typically a purchase or sales system would be divided into orders, deliveries, invoicing, recording in the accounting records and processing in the general & subsidiary ledgers.
- ▪
- Similarly a wages system is divided into appointments and discharges, hours worked, preparation of the payroll, wage disbursements and unclaimed wages.

2. Identify the **key documents or records** for each phase of the flow of information.

▪

3. For each document, identify the key information that should be recorded. This information is usually related to:
   - **Person**: the person with whom the client has entered into a transaction
   - **Price**: the price at which the transaction was entered into
   - **Quantity and description**: the quantity of the transaction entered into and the description of the goods and services

4. The following specific internal control objectives must be applied to all information in every document:

▪

- **Validity**
  - Must the information be **authorised**? If so, how and by whom?
  - Does the information represent an actual (valid) transaction with a bona fide third party? If so, who checks it, against what and how? - This is usually achieved by comparing the information with other documentation.
  - You need to indicate which information should be processed, by whom and whether a manual is required.

- **Accuracy**
  - Should the **information be checked** to see whether the amount is accurate? If so, how and by whom?
  - Should the information be processed to a specific account? If so, how does the client ensure that this is done?
  - You need to indicate which information or documents should be processed, by whom and whether a manual is required.

- **Completeness**
  - Are sequential documents used?
  - Who checks the numerical sequence?
  - Remember to state who the document should be sent to, who should check the numerical sequence and who should handle the missing items.

We shall illustrate steps 1-4 with the aid of an example before proceeding to step 5.

The following example relates to **credit sales**:

Step	Respective steps as set out in the above framework	Example relating to credit sales
1	Divide the system into **phases on the basis of the flow of information**	**Phase 1 of the credit sales cycle**: Client commits himself to a sales transaction
2	Identify the **key documents or records** for each phase of the flow of information	Order forms
3	Identify the key information that should be recorded for each document	The client's name, the selling price, discount, quantity and description of the goods
4	Apply specific control objectives for each piece of information on each document	**Validity**: The credit section must give permission on the basis of the client's credit-worthiness. The price must be compared with the price list. The document given must be agreed to the discount terms. Once all the above steps have been completed, the credit section would grant authorisation. **Accuracy**: The order form must be checked for accuracy by a senior person, in other words the selling price must be recalculated by multiplying the price with the quantity. **Completeness**: The inventory section must check the numerical sequence of the order forms and follow up any missing numbers.

5. In the recommended system you should always indicate **who** is responsible for carrying out the internal control, **how** the internal control should be carried out, **when** the internal control should be carried out, **what** internal control should be carried out and **on what documentation** the internal control should be carried out.

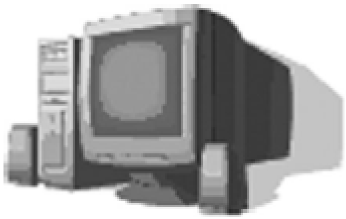
▪

6. Remember that in all cases the document must be **signed** as evvidence that the internal control has been carried out.

▪

7. Conclude by making certain that all the types of control activities in the entire system have been covered.
   - ★ The **approval / authorisation** of transactions;
   - ★ **Segregation of duties**, in other words, the distribution of core functions to different members of staff;
   - ★ **Isolation of responsibility**. Always remember to mention that a document must be signed as evidence that the internal controls have been carried out;
   - ★ **Access and custody controls**. For example, internal controls are required to ensure the safekeeping of assets and unused stationery;

- ★ **Comparison and reconciliation** – for example, the comparison of a creditors' statement with the creditors' account, and the performing of key reconciliations which are subject to management review;
- ★ **Performance reviews** – for example, review of the company's performance against the budget



Framework that can be used to design an internal control system for computerized systems

- ★ Systems modification controls are methods of ensuring that **authorisation** takes place, in other words, whether requests for systems modification are evaluated and authorised in advance by the user department and the information technology manager

▪

- ★ Batch controls are implemented mainly to ensure **accuracy**, although they also affect **validity** and **completeness**

▪

- ★ Regarding **completeness**, a computerised system usually assigns unique sequential numbers to transactions and carries out sequence checks to ensure that all transactions have been processed

General pitfalls in the design of an internal control system

The following shortcomings are often found in the design of an internal control system:

- ➢ Obvious principles of internal control are often omitted, such as that there must be adequate segregation of duties between the person who receives payments and the person who does the daily banking of cash.

▪

- ➢ Information supplied with the question is often not used. Always remember that the information given must be applied in your anwer.

▪

- ➢ Students often fail to give a full description of the necessary internal controls. Read the following two internal controls:

▪

- **Statement 1**: At the beginning of each week, the clerk must prepare a clock card for each employee from the permanent files, and issue these cards to the factory.

▪

- **Statement 2**: A clerk must prepare a clock card for each employee and issue it to the factory.

▪

There is an obvious difference between these two statements. Statement 2 does not contain sufficient detail. As stated above, it is always necessary to indicate **who** should carry out the internal control, **how** the internal control should be carried out, **when** the internal control should be carried out, **what** internal control should be carried out, and **on what documentation** the internal control should be carried out. See the following table for a further explanation:

Requirements	Statement 1	Statement 2
Who carries out the internal control?	The clerk	The clerk
How is the internal control carried out?	From the permanent files	**Missing – clearly indicates a lack of sufficient detail**
When is the internal control carried out?	At the beginning of each week	**Missing – clearly indicates a lack of sufficient detail**
What internal control is carried out?	Preparation of a clock card for each employee and issue of the cards to the factory	Preparation of a clock card for each employee and issue of the cards to the factory
On what documentation is the internal control carried out?	Clock cards	Clock cards

▪

Note that these questions (who, how, when, what and on what) cannot always be answered and included in your answer. Nevertheless it is a good idea to test each internal control that you write down against these questions, to see whether you have left out important details. Let us examine the followinng internal controls and test them against the requirements:

Unused cheque books must always be kept in a safe place by the cashiers

Requirements	Feedback
Who carries out the internal control?	The cashiers
How is the internal control carried out?	**This information is not provided & therefore this question cannot be answered**
When is the internal control carried out?	Always
What internal control is carried out?	Safekeeping
On what documentation is the internal control carried out?	Unused cheque books

Design of Internal Control Systems

The desing of internal control systems is illustrated by the following two activities.

Manual Systems

Activity

Your firm has been appointed the auditors of a primary school. An amount of R 1,5 million has been donated to the school by a well-known listed company in the engineering sector for the establishment of a sports centre on the school's premises. The sports centre includes two squash courts, two tennis courts, a swimming pool and a shooting range. The directors of the listed company have stipulated, however, that the project must be audited and that an appropriate auditor's report must be submitted to the directors upon completion of the project.

The headmaster is concerned about the required audit and wants to make sure that everything goes according to plan. He approaches you, as the partner in charge of the primary school's audit, and asks you to put together a plan showing how the project should be handled.

List the most important internal controls that the headmaster should implement regarding the establishment of the sports centre.

Feedback

1. A committee, and possible sub-comittee as well, should be appointed to take charge of the project

▪

2. A separate bank account should be opened and the R 1,5 million deposited into it. This account should be used exclusively for transactions relating to the project

▪

3. Two persons, one being the headmaster, should be authorised to sign cheques on this account

▪

4. An administrative official should be appointed by the committee. This person will be responsible for all the accounting and administrative functions

▪

5. Separate accounting records must be kept for the project. The most important record is the cashbook. The columns in the cashbook should make provision for the various sub-projects

▪

6. A bank reconciliation should be prepared monthly and submitted to the committee

▪

7. A detailed time schedule for the completion of the project should be drafted by the committee

▪

8. All meetings of the committee and sub-committees should be minuted

▪

9. Tenders for each project should be advertised in the local newspapers and in tender bulletins

▪

10. Only tenders from companies with a strong financial background and a good reputation should be considered.

▪

11. A tender may only be accepted after the committee has considered all the tenders received

▪

12. The acceptance of a tender should be accepted at a committee meeting. Committee members who have an interest in a particular tender should disclose such interest and should not take part in the voting on the tender in question

▪

13. Contracts with approved tenderers should be drawn up by a legal advisor appointed by the committee

▪

14. All documents should be placed in safekeeping by a responsible officer

▪

15. Each payment should be approved in writing by either the committee or the sub-committee, depending on the amount involved

▪

16. All relevant documentation and the written approval of the committee should be submitted to the headmaster before he signs a cheque

▪

17. The documents should be stamped “Paid” by the financial officer after payment has been made

▪

18. All cheques should be crossed

▪

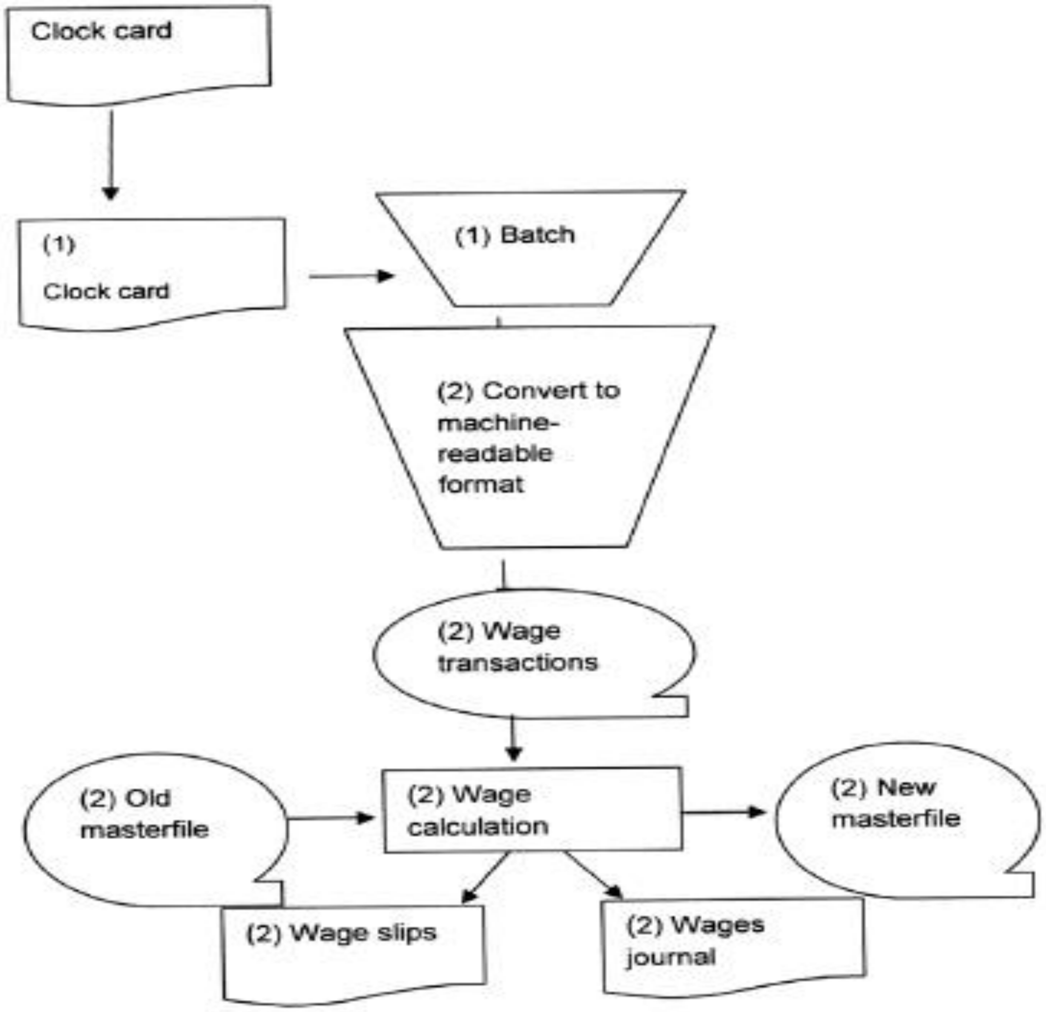
19. Unused cheque books should be kept in a safe place by a responsible person

▪

Computerised Systems

Activity

You are engaged in auditing the wages system at one of your clients. After extensive enquiries and observations, you have compiled the following simplified system flowchart:

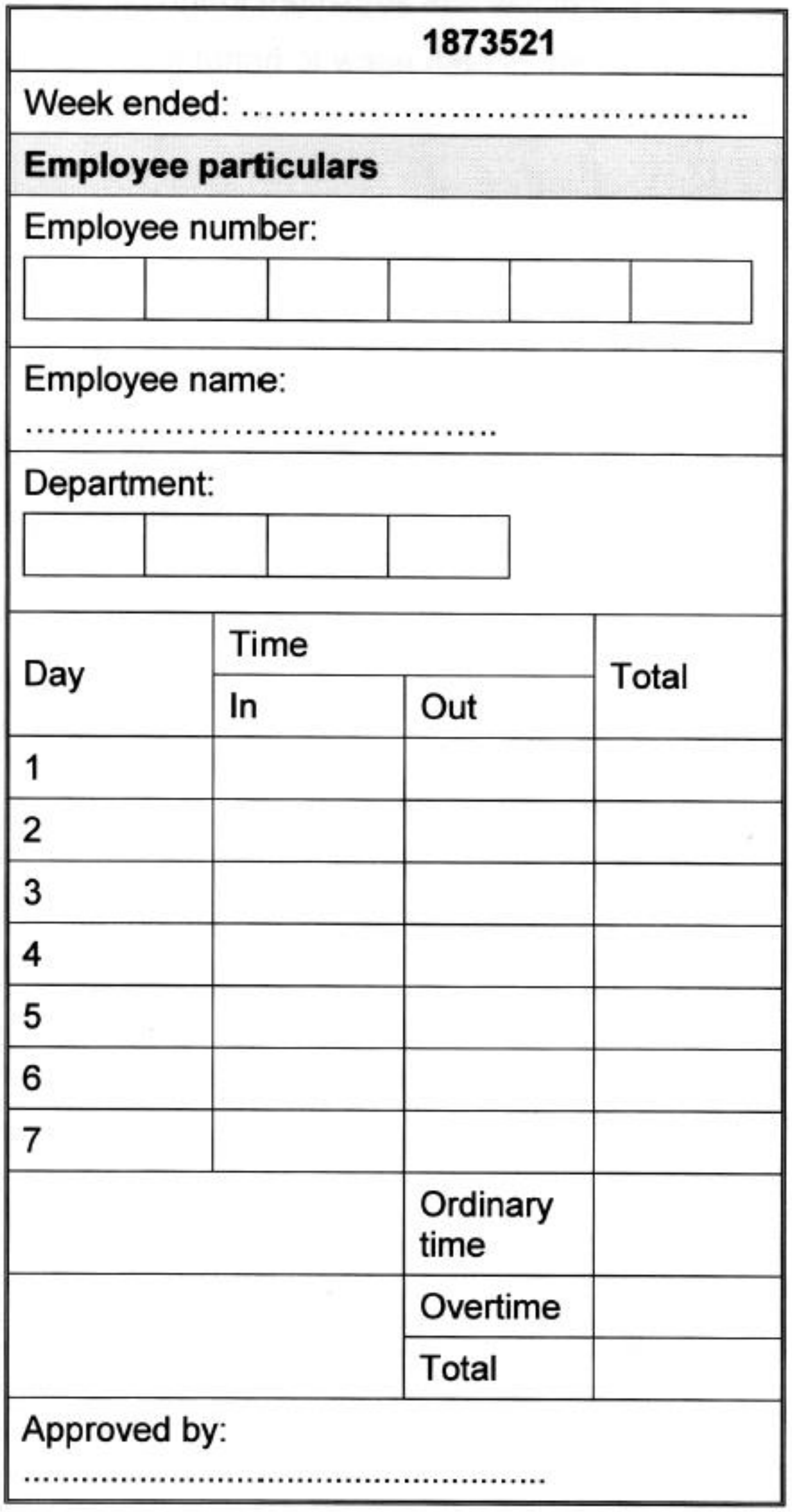


Note:

(a) Process takes place in the wages department

(b) Process takes place in the EDP department

The following specimen of a clock card used by the client was also supplied:



1873521

Week ended: ……………………………………….

Employee particulars

Employee number:

Employee name:

……………………………………….

Department:

Day	Time		Total
	In	Out	
1			
2			
3			
4			
5			
6			
7			
		Ordinary time	
		Overtime	
		Total	

Approved by:

……………………………………………………

Discuss the application control measures that would ensure the valid, complete and accurate capturing of wage data in the electronic data processing department

Feedback

Application controls within the EDP department to ensure the valid, complete and accurate input of wages data:

Data preparation

1. The EDP department acknowledges receipt of each batch by signing for it and recording the particulars of each batch in the batch register.

▪

2. The data input clerk receives the batches from the wages section and checks them as follows:

   ▪

   ★ He checks the particulars of the batch against the information on the batch control sheet;

   ▪

   ★ The numerical sequence of the clock cards is checked by test sampling and the data input clerk determines whether all the details on the clock cards have been completely and accurately filled in and whether the clock cards have been duly authorised;

   ▪

   ★ The data input clerk checks compliance with batch standards, namely that standard batch sizes have been used, a unique number has been allocated to each batch and control totals (both financial and hash totals) have been calculated;

3. Control totals must be recalculateed and must be agreed to the control totals recorded on the batch control sheet;

▪

4. Error handling: If any errors are detected as a result of the above checks & comparisons, the batch must be returned to the payroll section for rectification;

   ▪

5. The screen format must be standard and must be designed to make it easier to input information and reduce the possibility that mistakes will be made, e.g. the screen format could be made similar to that of a standard clock card;

   ▪

6. By means of on-screen dialogue, the computer must guide the input clerk through every stage of the input process;

   ▪

7. The computer must perform the following logical tests on the input fields during the input of data:

★ **Alphanumeric test**: to determine whether the input fields consist of the correct combination of alphabetical and/or numerical characters. The name of an employee can only consist of alphabetical characters, e.g. and the employee number can only consist of numerical characters

★ **Valid code test**: a code, such as the departmental code, is compared with a programmed list of valid codes for the payroll application

★ **Field size check**: to test whether each field contains the correct number of characters, for example that the employee number consists of six characters

★ **Sign test**: certain fields may only be positive & many not contain negative values, e.g. the number of hours worked per day and the total number of hours worked per week

★ **Limit test** : to make certain that certain input fields fall within predetermined limits, for example the total number of ordinary hours worked in a week may not exceed 40

▪

▪ A limit must also be placed on the total number of overtime hours worked. When this limit is exceeded, approval must be obtained in advance from a senior person, such as the manager of the wages section of a foreman.

8. During data preparation a check digit should be calculated for each field by the program and attached to the field.

▪

9. Error handling: the computer must display an error message as soon as an error is made during input. Errors must be corrected immediately. The system must be programmed to block further input until the error has been corrected.

▪

10. Computer-generated control totals must be agreed to the control totals in the batch register, after the input has been done for the conversion.

Batch input from the magnetic tape

1. The computer compares point-of-input control totals, which are balanced by the program after the input of each batch, with control totals calculated during data preparation.

▪

2. The system must recalculate the check digit for each field and compare it with the check digit attached to the field during data preparation.

▪

3. Logical tests must be performed on all the input fields.

▪

4. A sequence test must be carried out on fields and records during batch input to ensure that all fields and records are read in the correct sequence.

▪

5. Error handling: any errors that have been detected must be recorded by the computer in an error log. Error reports must be printed after each input run, but before processing has taken place. These reports must be checked and any errors corrected before a batch is processed.

The evaluation of internal control systems

General pitfalls relating to the evaluation of an internal control system

The following is a summary of the shortcomings generally encountered:

- ★ Obvious weaknesses are often left out. For example, management's failure to check calculations is often left out.
-
- ★ In questions that require students to describe the weakness and suggest a corrective measure, students do not properly explain how the weakness and the corrective measure are connected. For example, students state that order forms are not properly authorized before the order is placed with the supplier, but then as corrective measures for this weakness students sketch scenarios that bear no relation to the weakness. For example, they might say the following: ensure that there is sufficient separation of duties between the person who places the order and the person who approves it. It should be clear to you that the improvement suggested is not connected in any way to the identified weakness.
-
- ★ The above corrective measures for identified weaknesses often reveal a lack of detail, that is, students do not give a full description of the required internal controls. For example:
-
- Study the following two internal controls:
  - **<u>Statement 1</u>**: At the beginning of each week the clerk must prepare a clock card for each employee from the permanent files, and issue these cards to the factory.
  - **<u>Statement 2</u>**: A clerk must prepare a clock card for each employee and issue it to the factory

There is an obvious difference between these two statements. Statement 2 does not contain sufficient detail. As stated above, it is always necessary to indicate **who** should carry out the internal control, **how** the internal control should be carried out, **when** the internal control should be carried out, **what** internal control should be carried out, and **on what documentation** the internal control should be carried out.

Requirements	**Statement 1**	**Statement 2**
Who carries out the internal control?	The clerk	The clerk
How is the internal control carried out?	From the permanent files	**Missing – clearly indicates a lack of sufficient detail**
When is the internal control carried out?	At the beginning of each week	**Missing – clearly indicates a lack of sufficient detail**
What internal control is carried out?	Preparation of a clock card for each employee and issue of the cards to the factory	Preparation of a clock card for each employee and issue of the cards to the factory

On what documentation is the internal control carried out?	Clock cards	Clock cards

Basic guidelines that you may find useful in evaluating internal control system

The following guideline may be helpful if you find it difficult to evaluate the internal controls in the various transaction cycles:

Put yourself in the shoes of the owner of the business & then develop the internal controls that you would like to implement in your capacity as the owner.

As the owner of a business it would be important to you to introduce controls for dealing with risks. Suppose one of the risks in your business is that cheques received by post are not banked on account of theft. An essential control would therefore be that the post should be opened by two people, and the cheques recorded in a register. Unless this is done there is likelihood that a cheque could be stolen by a member of staff for personal gain. The result would be that you, the owner, would suffer a PERSONAL loss.

Evaluation of the internal control systems

The evaluation of internal control systems is illustrated by the following two activities:

MANUAL SYSTEMS

You are engaged in auditing the financial statements of Kasper de Bruyn, a large independent contractor. All his employees, most of whom are unskilled labourers, are paid in cash because Mr De Bruyn believes that this arrangement reduces administrative expenses and is preferred by the employees.

During the audit of the undertaking’s petty cash, you discover that the petty cash box contains almost R3000. You are informed that R 2500 of the amount represents unclaimed wages. On investigating this matter further you ascertain that Mr De Bruyn has ordered that any unclaimed wages be placed in the petty cash box so that the cash is available for future petty cash disbursements. When an employee appears to claim unpad wages he is immediately paid from the petty cash.
Mr De Bruyn informs you that this measure reduces the number of cheques drawn to replenish the petty cash fund. This also ensures that all the responsibility for cash on hand is vested in one person because the petty cash custodian always distributes the wage envelopes.

Required

Make a list of the internal controls that you would recommend to the client to improve internal control over both the wages and the unclaimed wages.

Feedback

1. Specific accounting procedures should be introduced for wages and unclaimed wages. A separate payroll bank account should be opened.

▪

2. Each wage envelope provided by the wages department should bear the employee's name and other relevant personal information about the employee.

▪

3. The wage envelope should be prepared by a person other than the person computing the payroll.

▪

4. Wage envelopes should be compared with the payroll records.

▪

5. Wages should be dealt with independently of petty cash or other cash receipts.

▪

6. The distribution of wage envelopes to employees should take place in the presence of a third, independent person.

▪

7. Every employee should sign for the receipt of his wage envelope.

▪

8. All unclaimed wages should immediately be handed to Mr De Bruyn or another independent person should be held in safekeeping until they are claimed.

▪

9. The unclaimed wages should be depositeed in the payroll bank account at regular intervals & the bank account should be reconciled regularly.

▪

10. The unclaimed wages account should be disclosed as a current liability on the balance sheet.

▪

11. The payment of any unclaimed wages from this bank account should be duly authorised.

▪

12. After a specified period, the unclaimed wages should be declared unclaimed and credited to wages.

▪

13. The petty cash should be maintained on an imprest basis, independent of any unclaimed wages.

▪

14. From time to time, on a surprise basis, Mr De Bruyn or any other supervisor should witness a payroll distribution.

COMPUTERISED SYSTEMS

Mrs De Beer has been working for BBP (Pty) Ltd for the past 12 years and is responsible for the salaries and debtors of the company. Mrs De Beer & the managing director, Mr Nel, have been personal friends for years and regularly go gambling at a casino near the offices of the company. They regularly use Mrs De Beer's computer password as their lucky number when they gamble. The board of directors have implicit trust in her because of her friendship with the managing director.

The annual salary increases are approved by the board of directors in March. After the meeting, a list prepared manually and showing all the approved salary increases is handed to Mrs De Beer, who captures the data on the computer. No employee of the company earns more than R 20 000 per month. After completing the changes on the computer, Mrs De Beer herself compares the information on the computer with the handwritten list. The list is then filed in Mr Nel's office.

The newly approved monthly salaries are as follows:

Mr Nel	R 19 500
Mr Roos	R 12 500
Mrs De Beer	R 9 500
Mrs Smit	R 4 500
Two other directors	R 19 500 each

The other 23 employees all earn a salary of between R 4 500 and R 7 500 per month.

At the end of each month Mrs De Beer prepares a payroll printout, but she does not check it. She gives the salary cheques, which are also printed by computer, and the payroll printout to Mr Roos, the accountant. Mr Roos totals the individual cheques and compares the total with that of the printout, unless he thinks the amount is more or less the same as that of the previous month. He then signs all the cheques, initials the printout and returns it to Mrs De Beer along with all the signed cheques. She deposits the cheques in the staff banka accounts.

Mrs Smit, who used to be responsible for all incoming post, resigned in May. Her work is now being done by Mrs De Beer.

At the end of June Mrs De Beer increased her own salary by R 4 500 and entered Mrs Smit's salary as a negative R 4 500 into the computer. Mrs De Beer printed two cheques for herself. They bore the same number, the one was for R 9 500 and the other for R 4 500.

In June Mr Nel used Mrs De Beer's password to gain access to the computer without her knowledge. He increased his salary to R 24 000 and also changed Mrs Smit's salary by minus R 4 500. Mrs De Beer tore up Mrs Smit's cheque for minus R 9 000 without looking at it and handed all the cheques to Mr Roos. The result was that the net amount of the salaries remained more or less the same.

Mrs De Beer did not realise that Mr Nel had made a change, because she printed the list of salaries & cheques and handed it to Mr Roos without checking it. Mr Roos did not notice the changes either, because the total of the salaries was more or less the same as for the previous month.

When Mr Nel tried to change his salary cheque back to R 19 500, he accidentally erased the debtors' masterfile. It took the company four months to reconstruct the debtors' masterfile.

Required

Identify the weaknesses in BBP (Pty) Ltd's internal control system and describe the internal controls that would eliminate these shortcomings.

Feedback

No	Weakness	Internal controls
1	No segregation of duties after Mrs Smit resigned. Mrs De Beer now opens all the incoming post and she is also responsible for debtors	Two people, other than Mrs De Beer, should open the incoming post to ensure proper segregation of duties
2	The changes in the salary masterfile were not reviewed by an independent person after Mrs De Beer did the changes for the annual salary increases	An independent person like the accountant should check the salary increases by comparing the handwritten list drawn up by the directors with the payroll masterfile. There should be proper segregation of duties
3	The use of Mrs De Beer's password as a lucky number when she and Mr Nel were gambling was a striking weakness	Passwords should always be kept confidential and not revealed to other people. Passwords should be changed regularly
4	Mr Roos does not compare each individual cheque with the payroll printout or examine the printout for abnormal items	Mr Roos should compare each individual cheque with the payroll prinout, or examine the printout for abnormal items. It would have been apparent that Mrs De Beer and Mr Nel had made out cheques for negative amounts
5	There are inadequate controls with regard to salary changes	Any change in the payroll masterfile should appear on the audit trail and should be approved by the directors
6	Mrs De Beer made out two cheques with the same number to herself	The making out of two cheques with the same number would have been prevented if the following controls had been in operation: • Sequence check • Control totals
7	Mrs De Beer and Mr Nel were able to make out a cheque for a negative amount	A sign test would have made it impossible to make out a cheque for a negative amount

8	Mr Nel increased his salary to R 24 000. The maximum salary that anyone can earn is R 20 000	A limit check would have prevented Mr Nel from increasing his salary to R 24 000
9	It took four months to reconstruct the debtors' masterfile	Proper backups and a proper plan would have reduced this period considerably
10.	There is no access control to the computer	The computer room should be locked & access should be controlled by means of keys and logs
11	The debtors' masterfile was erased	Boundary protection would have prevented the erasure. It would have prevented the payroll program interfering with the debtors' program
12	This company is not applying proper personnel practices	Personnel and their activities should be properly supervised to ensure that they are doing their work properly