Definition of Internal Control

- To address and limit potential risks
- designed, implemented and maintained by those charged with governance to provide reasonable assurance about the achievement of the company's objectives

Internal control address risks such as:

- safeguarding the assets of the company
- preventing fraud
- complying with laws and regulations
- producing reliable information
- operating the business effectively

Six key characteristics of internal control

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

Limitations of internal control

1. The cost on internal control must not exceed the benefit of it
2. Internal control is directed at routine transactions, not non-routine transactions
3. The potential for human error
4. The possibility of circumvention of internal controls
5. Possibility that a person responsible for internal control could abuse that power
6. Control procedures may become inadequate due to a change in conditions

Five components of internal control (CRICM)

1. Control Environment
2. Risk Assessment
3. Information systems
4. Control activities
5. Monitoring of controls

Control environment

- sets the tone of the entity and creates the atmosphere in which employees work
- employees at all levels must act with integrity and with a strong sense of ethics otherwise internal controls will not be effective
- if everyone knows what to do and how to do it, the control environment improves
- those charged with governance must also display commitment to ethical behavior
- there should be an effective organizational structure
- individual must be fully aware of the extent of their authority and how they exercise it
- sound policies regarding human resources should be in place

Risk assessment

- deals with how the entity assesses the risk and how they should be addressed
- board should ensure that risk assessments are performed on a continual basis
- IT risks form an integral part of risks assessment
- risk assessment process must be thorough, complete, accurate and comprehensive
- in order for this to work the objectives of the company must be clearly defined
- risks that threaten the achievements of the objectives can be identified and dealt with
- **Risk assessment involves the following:**
  - identifying risks relevant to objectives
  - assessing the likelihood/frequency of risks
  - estimating potential impact should the risk occur
  - deciding how to address the risk
- risk committees/officers may be appointed
- external risk consultants and risk models may be used
- **operational risks:** risk that threaten the achievement of effective/efficient operations
- **financial reporting risk:** risk that the entity will not achieve the objective of having an accounting system that records/processes only transactions which have occurred, are authorized, accurate and complete
- **compliance risk:** risk that the entity does not achieve objective of complying with the laws and regulations applicable
- management must put in place an information system + control activities

Control activities

- actions carried out to manage/reduce risks

Types of control activities (CAPSAI)

- Comparison and reconciliation
- Approval/authorization
- Performance reviews
- Segregation of duties
- Access/custody
- Isolation of responsibility

Control activities can be preventive, detective or corrective in nature:

- **preventive:** controls that minimizes errors/illegal events from occurring
- **detective:** designed to identify errors that slipped through the first round (bank recons)
- **corrective:** resolves errors identified by detective controls

Control activity vs. possible risk:

Control activity	Things that could go wrong (risks)
Comparison and reconciliation	Balance of cash receipts and payments journal could be incorrect if not regularly reconciled to the bank statement
Approval/ authorization	Credit sales could be made to customers who are not credit worthy, if the sale is not approved by the credit controller first
Performance reviews	Abnormal increase in transport costs due to fuel being stolen could go undetected due to management not comparing actual figure the budgeted figure
Segregation of duties	Goods purchased could be stolen if no segregation exists between the authorization and placement of the order and the issue of the goods received note
Access/custody	Physical inventory could be stolen if not stored properly
Isolation of responsibility	Incorrect number of goods could be received if a supplier delivers goods to a company and the receiving clerk doesn't count the goods and sign the supplier's delivery note

Difference between segregation of duties and isolation of responsibility

Segregation of duties is an internal control designed to reduce error and fraud by ensuring that at least two people are responsible for separate parts of a task.
Isolation of responsibilities refers to the accountability of an employee for a specific task, and acknowledgement by the employee for the performance of internal control. This is usually done by signing.

Monitoring of internal controls

- involves the assessment of internal control performance over time
- component of the process which tells management if the internal controls are working and if they re efficient

General Controls

- **D**: controls that establish an overall framework of control for computer activities
- they should be in place before any transaction processing is done

Categories of general controls

- **control environment:** communication + enforcement of integrity + ethical values commitment to competence, human resource policies and practice
- **system development & implementation controls:** in-house development, packaged software, program change controls
- **access control**
- **continuity of operations:** risk assessment, physical security, disaster recovery
- **system software and operating controls**
- **documentation**

Control Environment

- **Communication and enforcement of integrity & ethical values**
  - King III requires that ethical IT governance must be cultivated + promoted
  - ethical culture is important in IT department as they handle sensitive info
- **Commitment to competence**
  - demands of jobs in the IT department can be considerable

Participation by those charges with governance

  - according to King III< IT governance is the responsibility of the board: to provide leadership so that IT achieves the company's objectives
- **IT management's philosophy and operating style**
  - comes down to the attitude, control, awareness and actions of the IT management
- **Organizational structure and assignment of authority and responsibility**
  - should achieve 2 objectives:
    - establish clear reporting lines/levels of authority
    - lay the foundation for the segregation of duties
- **Human resource policies and practices**
  - will be the same as for other skilled personnel

System development and implementation controls

- unless the design and implementation of the system isn't carefully controlled, the cost of development may get out of control, the system design may not suit the needs of the user, programs may contain errors and bugs etc
- systems can be designed **in-house** or there can be made use of **packaged software**
- advantages of packaged software: lower cost, entire project is completed quicker, tech support is available, upgraded on a regular basis
- disadvantages of packaged software: may not meet company's needs, changes can't be made to the software, software developed overseas may not function in SA
- **program change controls:** aka program maintenance, programs must constantly be upgraded and modified
- all changes to programs should be effected by programmers, major change should be handled as a mini project etc

Access controls

- access to all aspects of the system must be controlled (hardware, software etc)
- **security policies** should be in place
- **physical access control**
- **logical access controls:** Identification (user name), authentication (passwords)
- passwords should be controlled (long, contain uppercase, lowercase, numeric etc)
- other access control: i.e. firewalls, etc

Continuity of operations

- aimed at protecting the IT facilities from natural disasters, destruction, attack, abuse
- **risk assessment:** assessing IT risk
- **physical security:** location, fire alarms, power surges etc
- **disaster recovery:** written plan how to recover, backups to be carried out frequently
- **other measures:** regular maintenance, adequate insurance, firewalls, anti-virus etc

System software and operating controls

- controls the use of hardware and application and end-user software
- **operating system software**
- **database management software**
- **system development software**
- **system support programs**

Documentation

- sound documentation policies are essential
- 2 objectives: all aspect of the computer system should be clearly documented, access to documentation should be restricted

Describe the general physical access controls that should be present to ensure proper internal control in a computerized environment:

- control over visitors from outside the company to the IT building
- controlled access to company personnel other than IT personnel
- physical entry to the data centre to be controlled
- access control over remote workstations

Give examples of preventative logical access controls in a computerized environment:

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

Explain what controls over passwords as part of logical access controls entails:

Passwords should be unique to each individual. Passwords should contain a minimum of 6 characters, and should not be easily guessed. They should contain a mix of upper and lower case, numeric and special characters. Passwords should be changed regularly. Passwords should never be displayed on pc's at any time. Personnel should not be allowed to exchange passwords with one another.

Application Controls

- an application is a set of procedures/programs design to satisfy the needs of users for a specific task
- any control within an application which contributes to the accurate and complete recording and processing of transactions that have actually occurred
- stages through which a transaction flows through the system: input, processing, output
- controls must also be implemented over master files
- objectives: revolves around the occurrence, auth, accuracy & completeness of data
- occurrence & auth are concerned with ensuring that data is not fictitious/fraudulent and are in accordance with the business activities and authorized by management
- accuracy is concerned with minimizing errors
- completeness is concerned with ensuring that no data is left out/incomplete

Control activities in a computerized accounting system

- **CAPSAIC**
- **Custody:**
  - application controls play a role in the custody of the company's assets held in electronic form (cash in bank)
  - must control unauthorized removals from the bank account
  - reconciliation of company records and bank statements
  - protect on line bank account
  - info on debtors held in the master file should be protected
  - data is protected by general and application controls
- **Approval and authorization**
  - the system can be programmed not to proceed if certain conditions/controls have not been satisfied
  - computerized systems are very effective in preventing unauthorized transactions from taking place
- **Performance reviews**
  - includes the review and analysis of actual performance against budgeted/previous
  - advantage of a computer system is that it can produce numerous useful reports
- **Segregation of duties**
  - danger in computerized system is that one employee has access to a lot of accounting records etc
  - segregation is achieved by controlling the access that employees have to system files
  - user profiles is set up
- **Access controls**
  - access to different applications can be constricted to different terminals
  - access is also restricted in terms of user profiles
  - physical access to PC's = general control
  - access at application level should be logged
  - the user must identify and authenticate himself to log in
- **Isolation of responsibility**
  - computer can be programmed to produce a log of who did what, when
  - access controls also contribute to isolation of responsibility
- **Comparisons and reconciliations**
  - recon and comparison is done between two different sets of information

Control techniques and application controls (BLOPS)

- **Batching**
  - controlling an activity which will be carried out on a batch of transactions
  - batching assists with: identifying data transcription errors, detection of data captured in incorrect fields, detection of invalid or omitted transactions or records
  - batch entry, batch processing/update
  - on-line entry, batch processing/update
  - on-line entry, real time processing/update
  - on line entry, batch processing/update
- **Logs and reports**
  - types of logs and reports include:
    - Audit trails - listings of transactions
    - Run-to-run balancing reports - o/b have been updated with transactions to deliver correct c/b

- Override reports - record of computer controls that have been overridden
- Exception reports - summary of any activities that falls outside the control
- Activity reports - provide record of all activity for a particular resource
- Access/Access violation reports - important for applications such as EFT/payroll

- **Output controls**
- purpose is to ensure that output is accurate and complete
- controls over distribution:
- clear report identification
- distribution matrix of who is to receive what, when
- hardcopy's movement should be controlled
- user controls:
- review of output for completeness
- reconciliation of output with input
- review of output for reasonableness

- **Program controls**
- controls built into application software to validate information
- existence/validity checks
- reasonableness and limit checks
- dependency checks
- format checks
- check digits
- sequence checks
- program edit checks
- program reconciliation checks

- **Screen aids and related features**
- all the features reflected on the screen to assist the user
- minimum keying in of information
- screen should be formatted as the hardcopy would look
- use of screen dialogues and prompts
- mandatory fields
- shading of fields

Master file amendments

- objectives of application control over master files:
- only valid amendments are made to master files
- details of the amendment are captured and processed accurately
- al master file amendments are captured and processed
- steps:
- Record all master file amendments on a source document
- authorize master file amendment forms
- enter only authorized master file amendments
- review amendments to ensure that they occurred and were authorized

The entity's internal control from perspective of external auditor

- consider the 5 components again:
1. Control Environment
2. Risk Assessment
3. Information system
4. Control activities
5. Monitoring of controls

Control environment

- communication and enforcement of good ethical values
- commitment by management to competent performance
- management's philosophy and operating style
- organizational structure provides a clear framework and clearly defines authority and responsibility
- evidence about the control environment can be gathered by:
  - observation of management and employees
  - inquiry of management
  - inspection of documents

Risk Assessment process

- identifying business risks
- estimating the significance of risks
- assessing the likelihood of the risk occurring
- responding to the risk
- information about the process can be gathered by
  - inquiry
  - inspection of documentation

Information system

- auditor must obtain an understanding of classes of transactions
- procedures by which transactions are initiated, recorded, processed and corrected
- related accounting records and supporting docs
- how the system captures events
- process used to prepare financials
- controls over passing of non-standard journal entries
- manner in which financials are conveyed to management
- computerized applications
- hardware and software
- complexities of the system
- information on the system can be gathered by inspection, observation, inquiry, discussion with employees and prior year audit staff and tracing of transactions

Control activities

- policies that ensure that management's objectives are carried out
- authorization of transactions
- segregation of duties
- physical control
- comparison and reconciliation
- access controls
- custody controls
- good document design
- general and application controls in IT systems
- information on the activities can be gathered by: inspection, observation and inquiry

Monitoring of controls

- tells management how the controls are doing over time
- looks at all the components of the internal control process
- information about monitoring can be obtained by: inquiry and inspecting

Significant risks

- risks that require special audit consideration
- relate to the auditor's risk of material misstatement
- auditor identifies and assesses the risk so that he can determine the nature, timing and extent of any further audit procedures

Six factors the auditor should consider when assessing whether a risk is significant

1. Whether it is a risk of fraud
2. The complexity of the transactions
3. Whether the risk is related to recent significant economic/accounting developments
4. Whether the risk involves significant transactions with related parties
5. The degree of subjectivity in the measurement of the financial info related to the risk
6. Whether the risk involves significant transactions outside the normal course of business