AUE 2602

HOMEWORK 2 - MEMORANDUM

INTERNAL CONTROLS
(About + 15 – 20 marks in Exam)
Jackson Chapter 5 & 8

QUESTION 1: INTERNAL CONTROLS : (ASSIGNEMENT 3 - 2010)

REQUIRED:

1.1 Describe 6 ***Characteristics*** of good internal Controls (71/2)

1,2 Describe ***3 Methods*** whereby an Auditor can obtain an understanding of a company's internal control system. (4 ½)

1.3 List ***5 Factors of which*** the auditor should be aware of, when computer information systems are used, instead of manual systems (5)

1.4 List ***5 Components*** of Internal Control (5)

1.5 List ***four (4) inherent limitations*** of internal control. (4)

QUESTION 1 : ANSWERS

1.1 Characteristics of good internal control: (Jackson Ch 5/4 & 5/7 & 8/6)

- ***Internal control is a process***
- ***Internal control is affected by people and paper***
- ***IC is not the sole responsibility of management***
- ***IC is not static***
- ***IC is not foolproof***
- ***IC is not a case of a single control addressing a single risk***

When considering these characteristics we address the risks associated in the following:

1 ***Control environment*** - The control environment sets the lone of the organisation and influences the control consciousness of its staff. To ensure a strong control environment, it is essential that management leads by example and through their actions and behaviour in order to promote an environment in which adherence to controls is regarded as very important.

2 ***Competent, trustworthy staff*** - People are a fundamental component of internal control. Personnel involved in the internal control system should be competent to fulfil their functions honestly and reliably. Without competent, trustworthy personnel, the best internal controls can be circumvented.

3 ***Segregation (division) of duties*** - Within an organisation there should be segregation of duties between the people responsible for the functions of authorisation, execution and recording of transactions and custody of assets.

4 ***Isolation of responsibility*** - Employees should be fully aware of their responsibilities and must be held accountable for their actions. It is important that employees acknowledge in writing (by means of a signature) that they have performed a certain task to fulfil their responsibility. This isolates employees responsible for carrying out a task and isolates the transfer of responsibility from one

person to another.

5 ***Access/custody controls*** - It is important for the organisation's assets to be protected against damage, unauthorised use and theft or loss at all times. This protection not only relates to physical assets of the organisation such as, stock or plant and equipment, but also to cash, investments and debtors.

6 ***Source document design*** - Properly designed source documents can assist in achieving good internal control and will promote the accuracy and completeness of recording transactions. Source documents should be pre- printed, pre-numbered, multi-copied and designed in a logical and simple manner.

7 ***Comparison and reconciliation*** - Independent comparison and reconciliation should take place frequently and timely. Senior personnel should review reconciliations and ensure that all reconciling items are followed up.

1.2 Methods to obtain an understanding of an internal control system

(Jackson: Ch 7 / pg 12 or SG 142 Observation, Inpection etc.)

1. ***System walk-through tests*** - This is'the process where an auditor selects a number of documents by which a certain transaction type is initiated and then follows the trail through the entire accounting process.

2. ***Enquiries and discussions*** - Meetings can be scheduled with management and the staff so that Lhey can give the auditor information on the internal controls in the various transaction cycles.

3. ***Inspection of documentation*** - The auditor could study various documents in order to obtain an understanding of the internal controls present in the various transaction cycles.

4. ***Observation of internal controls and processes*** - Internal controls and processes can be observed by the auditor.

5. ***Internal control questionnaires*** - Auditors can design an internal control questionnaire (ICQ) to identify the expected internal controls which is then used to document the internal control system. However, an ICQ contributes to an auditor's understanding of the design and functioning of the internal control structure, but does not contribute to an understanding of effectiveness.

1.3 Factors which the auditor should be aware of when computer information systems are used

(Jackson: Ch 7 /12 Ch 8 / pg 8 Reliance on the system, Unauthorised access, IT Personal gaining access etc)

1. Lack of transaction (audit) trail.
2. Lack of segregation of duties.
3. Potential for errors and irregularities.
4. Automatic initiation or execution of transactions.
5. Dependence of other controls on computer processing.
6. Uniform processing of transactions.
7. Potential for increased management supervision.

1.4 Components of Internal Control - NB!!!

1. Control Environment
2. Risk Assessment process
3, Information System,
4, Control Activitities,
5. Monitoring controls

1.5 List 6 inherent limitations of internal control. (4)

Cost of internal control exceeds the benefit
Only directed at mostly Routine transactions.
Human error.
Collusion of management or employees
Abuse of responsibility and the system

Due to changes, the sustem may become inadequate

GENERAL CONTROLS IN AN EDP SYSTEM

QUESTION 1: General Controls (Assignment 3- 2010) (12 marks)

You have been appointed the auditor of a client that uses an electronic data processing system.

The client's revenue consists mainly of credit sales to customers. They make use of a data base system for their debtors, and credit limits are carefully monitored.

Master files are kept of all debtors and strict internal control of any changes to the master files are adhered to.

YOU ARE REQUIRED:

1.1 To briefly name and describe the main 8 categories of *general controls* that should be in place in a computerized environment . (12)

ANSWER:

1.1

- Control environment and security policy
- Organisational structure and Personal practices
- Standards & standard operating controls
- Systems development control & Systems software controls
- Programme/ systems changes controls
- Continuity of operations
- Access Controls to data and programmes
- Documentation

1.1 *Categories of general Controls in EDP System:* (Jackson : Ch 5 / pg 7 & Ch 8 /pg6)

1. Control environment and security policy

- The control environment sets the tone of the organisation and influences the control consciousness of its staff. To ensure a strong control environment, it is essential that management leads by example and through their actions and behaviour in order to promote an environment in which adherence to controls is regarded as very important.
- A security policy deals with the security standards that management needs to comply with in order to maintain the integrity of the hardware and software used in the organisation. The policy should be documented and should be based on principles rather than detailed procedures. Logging, defence in depth, fail safe and least privilege are some of the principles to be included in a security policy.

2. Organisational structure and personnel practices

- Organisational structure should lay the foundation for segregation of duties and establish dear reporting lines.
- Management should institute personnel practices that will ensure that the organisation recruits honest, competent and trustworthy personnel.

3. ***Standards and standard operating procedures***

- Computerised systems should be managed according to predetermined conventions, protocols and standards, for example the ISO 9000 series.

- Standard operating procedures are those procedures setting out the "day-to-day" operations in a organisation which include equipment operation and maintenance, machine servicing, job run procedures, scheduling of jobs, etc.

4. Systems development controls

- Systems development refers to the development of a new computer system for the entity which could be purchased or developed in-house. If all the system development controls are complied with, chances will increase that the system will operate reliably when completed.

5. Program change controls

- Program change controls describes changes to a system after implementation, with the purpose of correcting errors or meeting the changing needs of users. Controls must be implemented to ensure that changes are authorised and are made in an effective manner.

6. Continuity of operations

- These controls are aimed at protecting computer facilities from natural disasters and acts of destruction, attacks or abuse by unauthorised people. Poor controls result in disruptions in normal processing.

7. Access controls

- Only authorised users should be allowed access to computer facilities and data, in order to prevent damage and theft of equipment as well as manipulation, destruction or theft of data.

8. Documentation

- Sound documentation policies are essential in order to improve overall operating efficiency, provide audit evidence, improve communication at all levels, avoid undue reliance on key personnel, and train users when systems are initially implemented.

1.2 To name three alternative methods of input of credit sales transactions. (3)

1.2 Answer:

- Batch input/ batch processing function.
- On- Line input/ batch processing function
- On-Line input/ Real-time processing
  (3)

QUESTION 2: GENERAL CONTROLS: System Development controls (Assignment 3: 2010)

You are the auditor of MNO (Pty) Limited. The company decided to develop a New inventory system and prepared written standard procedures to control the development of the new system. Management submitted the following written standard procedures for your comments before commencement of the system development process.

PROJECT PLAN For DEVELOPMENT OF NEW INVENTORY SYSTEM:

1. The Users, accounting personnel and the internal auditors must be contacted to participate in the system development process.
2. Management, the users and the internal auditors must review the work accomplished during the system development process.
3. Management and the users and the internal auditors must approve the system development proves at the end of the process.
4. The system testing must be limited to the computerized phase.
5. The approval will be given by means of passwords. The passwords are pinned to the notice board in the different departments.

6. The conversion process will take place immediately after the sytem is approved.
7. The system will be implemented after the final approval. No post implementation review is planned..

REQUIRED:
Suggest improvement for each of the shortcomings in the project management plan of MNO (Pty) Limited. (10)

QUESTION 2: ANSWERS:

Improvements with regard To project management plan

1. The external Auditor must also be contacted to participate in the system development process.
2. The System Supervisors must review the work of the systems staff on a technical level.
3. The SDP must be approved at the end of each phase of the SDP.
4. The System testing should include all aspects of a system and should include both the manual phase and the computerised phase.
5. Passwords should be strictly controlled and should not be disclosed to other staff.
6. Fole conversion approval should be given before the conversion process begins.
7. A post-implementation review should be conducted a few months after implementation of the system.

Should be: System Developer, Analyst & Project Team

QUESTION 3: Gen Controls – Personnel Practices (Assignment 3 – 2010)

"People" are the most important part of any control system. Characteristics of honesty, competence and trustworthiness are essential in a computerised environment and management should therefore institute good personnel practises.

REQUIRED:
Describe 4 Personnel practises to be incorporated in the company's standard operating procedure to ensure that good personnel practices are applied throughout. (6)

ANSWER: QUESTION 3

1. An entity should have ***proper recruitment policies*** so as to ensure that honest and competent employees are appointed. This will include:
   - Conducting of interviews.
   - Tests that should be written.
   - Background checks.
   - Evidence of qualifications should be followed up and investigated.
   - Contacting of references.
2. ***Immediate exclusion from computer facilities*** if an employee is dismissed,for example passwords and other privileges should be cancelled.
3. **Compulsory leave** - special arrangements should be made if personnel lake annual or sick leave. Staff should also be encouraged to take leave on a regular basis, as staff who are involved in unauthorised activity will often be uncovered when they are not present to cover their tasks.
4. ***Training and development should*** be offered to staff. They should attend courses and seminars in order to keep them up to date and fulfil their functions efficiently and effectively.
5. **Written formalisation of personnel *practices in a guideline***. These guidelines should be accessible to all staff to provide employees with terms of reference or guidelines. The guideline should be reviewed on a regular basis.
6. ***Rotation of duties*** - moving employees between functions is a useful personnel practice as it helps avoid undue reliance on any individuals by ensuring that each employee has a backup. It may also relieve boredom (and cut down on human error) as well as encourage employees to develop new skills. (9)

QUESTION 4 : GENERAL CONTROLS: Specific Risks : (Assignment 2: 2009)

Recently, your firm was appointed as the auditors of AAA (Pty) Limited. The company uses information technology systems for their financial reporting as well as for operational purposes. They contacted you regarding the specific risks to their internal control posed by information technology.

REQUIRED:

Write a *memorandum* to the Chief Executive Officer of AAA (Pty) Limited, in which you indicate six (6) specific risks that information technology poses to the company's internal control. (10)

ANSWER: QUESTION 4

INTERNAL CONTROL MEMORANDUM

Memorandum: Specific risks to internal control posed by information technology

To: The Chief Executive Officer of Local Architects (Pty) Limited

From: CCK Auditors

Specific Risks to Local Architects (Pty) Limited's internal control posed by information technology" includes:

1. Reliance on systems or programs that are inaccurately processing data, processing incorrect data, or both.
2. Unauthorised access to data that may result in destruction of data or improper changes to data, including the recording of unauthorised or non-existent transactions, or inaccurate recording of transactions. (Particular risks may arise where multiple
3. The possibility of information technology personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.
4. Unauthorised changes to data in master files.
5. Unauthorised changes to systems or programs.
6. Failure to make necessary changes to systems or programs.
7. Lack of manual controls during computer processing.
8. Potential loss of data or inability to access data as required (viruses/use of discs/data can be destroyed).

NB!!!!

QUESTION 5: General Controls – (Assignment 2- 2010)

Your Client, ABC Engineers (Pty) Limited, has computerised its general ledger, debtors, creditors and inventory control systems during the year. For this purpose an EDP department has been established.

Name:	Position
Mr Samuals	EDP Manager
Mr Grey	Programmer
Mr Mombeni	Librarian
Ms Jee	Data Clerk
Ms van Tonder	Data Clerk
Mr Steward	Data Clerk

Mr Samuals is responsible for appointing new staff members, after having conducted interviews with them. He is also responsible for solving problems that arise within the EDP department.

Mr Grey is responsible for drawing up specifications for new systems (when required). He also makes changes or adjustments to the existing system on telephonic requests from systems users; designs new systems and tests program changes; writes manuals and updates program documentation.

Mr Mombeni stores all company data files by locking them in the safe at the end of each day, after he has walked through the whole department and collected all discs.

The data clerks prepare data for computer processing and enter the data.

The managing director of the company, Mr Smith, asks you to review the ***General Controls*** of the EDP Department.

REQUIRED:

5.1 Describe 8 controls which would prevent unauthorised persons from using ***the terminals***. Your answer should deal with ***physical*** and ***logical*** controls. (12)

5.2 Write a memorandum to the managing director ABC Engineers (Pty) Limited, Mr Smith, in which you indicate ***4 weaknesses*** in the existing ***General Controls*** of the EDP department, with reference to the available information. (6)

ANSWER: QUESTION 5

5.1

Controls which will prevent unauthorised use of terminals

PHYSICAL ACCESS CONTROLS:

- **Security checks** should he performed on visitor's identity and purpose of visit by the guard at the gate, before they are allowed entry to the property and premises within which terminals are housed.
- Visitors' **arrival (and later departure**) **should be logged** and they should be given an Identification tag.
- Visitors should be ***verbally directed*** or escorted to terminals because it is (intentionally) not clearly marked. .
- Doors to the room containing terminals should be locked to prevent ***unauthorised people*** **from** ***gaining*** *access.* To enter, you need a key. Swipe card, code number of combination of these, which deactivates the lock.
- ***Cabling should*** *be shielded* or built Into walls to prevent line tapping.
- A ***surveillance camera*** should record arrival of people at the facility.
- People should not be allowed into the computer room which houses the ***central processing unit****.*

LOGIC ACCESS CONTROLS

Once staff members switch on their terminals:

- A screen prompt should require them to enter their user IDs.
- Although the system recognises a staff member as an authorised user, it should require them to enter their passwords and possibly other personal information.
- A menu tailored specifically for a staff member should appear on the screen, providing the staff members to access only those particular modules which they need in order to perform their duties.

5.2

INTERNAL CONTROL MEMORANDUM

Memorandum: Weaknesses in the existing general controls of the EDP department

To: The managing director of 3CS Engineering (Pty) Ltd

From: XYZ Auditors

Date: 31/08/2009

Weaknesses in the existing genera! controls of the EDP department include:

1. Except for the conducting of interviews by the EDP manager, it seems as if there is a lack of formal and proper recruiting policies, which include careful checks on an applicant's background and competence.
2. Requests for program changes are made by telephone - there is no written authorisation or independent investigation into the necessity, costs etc. involved in such changes.
3. It is clear that there is a lack of a formal systems development methodology in which duties are segregated, deadlines are set and responsibilities are fixed.
4. It appears that the library function occurs informally - the librarian walks around the department and collects all discs. This point to a lack of formal authorisation and control over the issuing and return of data files.

QUESTION 6 – Program Development – Changes (Assignment 3 – 2010)

You are the auditor of LA (Pty) Limited. The Company is the 3rd largest tequi;a producer and distributer in SA and operates throughout the country.
The Company uses a large number of computer programs, all of which have been developed internally and are maintained by company personnel. During the performance of the interim audit, you were handed a detailed description of the company's system for program changes.

The Following extract comes from that description:

1. Requests for changes to the current system are originated by either the users or development personnel.
2. The requests for changes to the system are made via telephone to the data processing manager , Mr Cuerva.
3. After Mr. Cuerva has received the request, he holds a meeting in his office, with the person who originated the request and verbally approves it.
4. During the project development, development personnel are encouraged to report back to Mr. Cuerva about the progress of the project.
5. After the changes are completed, they are checked by Mr. Cuerva and he gives his final approval for the changes.
6. The changes are tested and implemented by the development personnel over a weekend so as not to disrupt personnel working on the programme.
7. Mr. Cuerva reviews the test results and if he is satisfied he personally updates the system documentation. He informs the personnel by preparing a short description of the changes and forwards this via e-mail to all the relevant personnel, the users and the internal audit department.
8. A copy of the description is printed and filed in the library together with the rest of the documentation. Thereafter personnel may continue normal processing on the program.

REQUIRED:
List *the shortcomings* in the Program Development of the System and describe the controls which would improve the program development of the system. (12)

Present your answer in the following format:

Shortcoming	Control which would improve the program development of the system
1.	1.

ANSWERS: QUESTION67

Shortcoming	Control which would improve the program development of the system
1. Verbal requests for program changes.	1. Program change requests must be done in writing.
2. No formal approval of program changes by the users and internal auditors.	2. Program changes must be approved by the users and internal auditors before Mr Cuervo approves them.
3. System development methodology is not followed during system development.	3- System development methodology should be followed when making changes to systems.
4. Changes are made directly to the current programs.	4. Changes should be made to programs after copies of the original programs have been made and safely stored in the library.
5. Test results are not approved by the users and internal auditors.	5. Test results must be approved by the users and internal auditors before Mr Cuervo approves the changes.
6. No proper documentation of system changes.	6. System changes should be properly documented, as detailed documentation is required.
7. No follow-up testing is done to ensure that all authorised changes are effected and functioning properly.	7. A post-implementation review needs to be conducted on the system.
8. No training of users after the changes have been implemented.	8. Users and operators need to be retrained on the system after the changes have been implemented.

QUESTION 8: Access Controls (30 marks)

Computer systems have the following characteristics which may pose a problem for the auditor:

Direct access to the computer by various users
Immediate processing of data input
The absence of a permanent record for all data captured and processed.

You are required:

9.1 To discuss the controls that should be in place to ensure that *only authorized personnel gain access* to the computer data files. (12)

QUESTION 8: ANSWERS:

a) Control over Physical access to the computer

Lock computer room
Only authorized personnel may enter

Lock computer when not in use
Maintain logs of users
Review logs regularly

b) Control over physical access to computer data files

Files in custody of a person independent of persons who use the computer
Files only issued to authorized personnel
Record to be kept of file record issues

c) Control over the use of the programme

Use of passwords
Passwords to be amended frequently (12)

QUESTION 9: General Controls

Your client ABC Limited, has recently established an electronic data processing department, which incorporates the computerization of accounts receivable and accounts payable.

The organizational structure of the EDP department at present is: an EDP manager, A control clerk, input operators, a programmer and a librarian.

There are five computer terminals in the EDP department and they are linked online to the mainframe computer which is situated in the office of the computer manager.

The computer manager is responsible for appointing new staff members, after interviews have been conducted with them as well as solving problems in the EDP department.

The computer programmer is responsible for the following:

- Drawing up systems specifications for new systems, when required.
- Making changes and adjustments to the existing system on the basis of telephone requests from the users and operators
- Designing and testing new systems and program changes

The control clerk receives all data for input and processing from the user departments.
He also distributes the printout and output documents by handing them over to a messenger for distribution to the relevant departments.
He also updates the Data Base system for Accounts Receivable.

At the end of each day, the librarian collects all disks and files each day and stores all data files by locking them in a safe. The librarian also acts as assistant programmer at times when the work load of the programmer becomes too much.

The input operators prepare data for processing and enter the data on the computer.

New staff members must be appointed in the near future due to expansion.

Required:

To identify the *weaknesses* in the *general electronic data processing controls* of ABC (Pty) Limited and *make recommendations* for these controls. (25)

ANSWERS: QUESTION 9

Weaknesses	Recommendation
Appointments ○ Except for personal interviews there is a lack of formal and proper appointment procedures	○ Must do background tests ○ No investigation if skilled for the job. (perform in-house evaluations) ○ Contact former employer
The programmer ○ designs and tests new systems ○ As well as program changes ○ There is a lack of segregation of duties	○ Manager should be responsible for system design only ○ Program changes should only be implemented by formal request and validity checks
○ Requests for program changes are made telephonically	○ Must be written requests and authorization ○ Independent investigation into necessity of changes ○ Evaluation of the costs involved
Control clerk ○ does not carry out any procedures to test controls on data received ○ or processed ○ Or on the results from processing	○ Must make sure that Input data is prepared properly ○ Processed properly (errors to be returned for correction) ○ And results should be checked with control totals and hash totals
The System Manager ○ Does not oversee the system controls (programmer does) ○ Programmer designs policy and procedure manual (no separation of duties) ○ No distinction between system and application controls.	○ He should be in charge of the design of the system ○ He should update policy and procedure manuals (not the programmer) – Separation of duties ○ Systems manager in charge of general controls and programmer to be in charge of application controls
The Librarian ○ Also acts as assistant programmer ○ Only stores data files and not other software programs or documentation of the company ○ Librarian informally collects disks	○ Must be segregation of duties and not be involved with programming. ○ Must take control of all files, system software and output ○ Should keep a register of what comes into and what goes out of library(authorization) ○ Should make sure every file is properly labeled and correct and not damaged or corrupt.
Operators ○ They prepare input data and process the input of data	○ Should be separation of duty and not do both functions

(**to any 25 marks)**

QUESTION 10 - ACCESS CONTROLS (Assignment 2 – 2011)

Your client, Bounce Back Limited, a manufacturer of soccer balls, has recently won the 2011 Soccer World Cup tender to supply soccer balls for all the tournament games. The company was recently established by two brothers, Oriando and Pirates.

Since the establishment of the company, the owners, Orlando and Pirates, have computerised all their operational systems which consist of five modules, namely purchasing, manufacturing, distribution, finance and statistics. All of these modules are fully utilised, except for the statistics module which provides valuable information and graphs regarding the manufacturing process.

The tender requirements included, amongst others, the provision of quarterly manufacturing statistics to the organising committee of the 2011 Soccer World Cup.

To meet the strict-tender requirements, Orlando and Pirates decided to appoint two new staff members to calculate, report on and draw graphs for the quarterly manufacturing statistics. Orlando and Pirates are concerned that manufacturing statistics may be manipulated, destroyed or stolen by unauthorised people.

REQUIRED Marks

Describe five (5) general access controls that should be Implemented by Bounce Back Limited to prevent manufacturing statistics from being manipulated, destroyed or stolen by unauthorised people. Your answer should deal with physical and logical access controls. (71/2)

QUESTION 10 : ANSWER

Physical access controls

- Security checks should be performed on a visitor's identity and purpose of visit by the guard at the gate, before the visitor is allowed entry to the property and premises within which the computer facilities are housed.
- Visitors' arrival (and later departure) should be logged and they should be given an identification tag.
- Visitors should be verbally directed or escorted to the computer facility because it is (intentionally) not clearly marked.
- Doors to the room containing computer facilities should be locked to prevent unauthorised people from gaining access. To enter, you need a key, swipe card, code number or combination of these, which deactivates the lock.
- Cabling should be shielded or built into walls to prevent line tapping.
- A surveillance camera should record the arrival of people at the facility.
- People should not be allowed into the computer room which houses the central processing unit.

Logical access controls

Once staff members switch on their personal computers the following should take

- A screen prompt should require them to enter their user IDs.
- Although the system recognises staff members as authorised users, it should require them to enter their passwords and possibly other personal information.
- A menu tailored specifically for staff members should appear on the screen, providing the staff members to access only those particular modules which they need in order to perform their duties.

QUESTION 11 – June 2013 Exam

1.2 Describe the **general physical access controls** that Minetech should implement to control **access to the computer** onto which the company's internet banking software is loaded in a **computerised environment**. **(15)**

1.3 Describe the **password controls** as part of good logical access control that Minetech should implement to prevent the theft of money due to unauthorised access to the company's bank account in a **computerised environment.**
Note that your answer should only address password controls. **(10)**

QUESTION 11 - MEMO: (June 20`13 – Exam) (No specific Q Nov 2013)

1.2 General physical access controls to prevent access to the computer onto which the company's bank account software is loaded 15 marks

Reference: - Jackson and Stent (2012: 8/17-8/18)

1. The IT department should be contained in a separate building or wing of a building. (1½)
2. The building should have a dedicated room in which all the equipment which runs the system would be housed, for example the CPU and servers. (1½)
3. Only a limited number of personnel should be allowed access to the data centre. (1½)
4. Visitors from outside the company to the IT building should be controlled (1½) :
   - be required to have an official appointment to visit IT personnel working in the IT department. (1½)
   - on arrival be cleared at the entrance to the company's premises, for example by a phone call to the IT department. (1½)
   - be given an ID tag and possibly escorted to the department. (1½)
   - not be able to gain access through the locked door. (1½)
   - wait in reception (or be met at the door) for whoever they have come to see. (1½)
   - be escorted by a security guard out of the department at the conclusion of their business. (1½)
5. Entry to the data centre by company personnel other than IT personnel should be controlled. (1½)
6. Physical entry to the data centre (dedicated room) should be controlled (1½) :
   - only individuals who need access to the data centre should be able to gain entry. (1½)
   - access points should be limited to one. (1½)
   - access should be through a door which is locked. (1½)
   - the locking device should be de-activated only by swipe card, entry of a PIN number or scanning of biometric data. (1½)
   - entry/exit point should be under closed circuit TV. (1½)

   (Remember the data centre is the heart of the company's information system.)
7. Remote workstations/terminals should be controlled: (1½)

- should be locked and secured to the desk. (1½)
- placed where they are visible and not near a window. (1½)
- offices should be locked at night and at weekends. (1½)
- Data cables should be protected to prevent tapping as a means of access to the system. (1½)

(1½ for each valid point to the max. of 15 marks, available 31.5 marks)

1.3 Password control to prevent unauthorised access to the company's bank account 10 marks

Reference: - Jackson and Stent (2012: 8/20)

1. Passwords should be unique to each individual. (1½)
2. Passwords should consist of at least six characters, be random not obvious, and a mix of letters, numbers, upper/lower case and symbols. (1½)
3. Passwords/user-ID's for terminated or transferred personnel should be removed/disabled at the time of termination or transfer. (1½)
4. Passwords should be changed regularly and users should be forced by the system, to change their password. (1½)
5. The first time a new employee accesses the system, he/she should be prompted to change his initial password. (1½)
6. Passwords should not be displayed on PCs at any time, be printed on any reports or logged in transaction logs. (1½)
7. Password files should be subject to strict access controls to protect them from unauthorised read and write access. (1½)
8. Personnel should be prohibited from disclosing their passwords to others and subjected to disciplinary measures should they do so. (1½)
9. Passwords should be changed if confidentiality has been violated, or violation is expected. (1½)
10. Passwords should not be obvious, e.g. birthdays, names and name backwards. (1½)
11. Two passwords from two separate personnel should be required to gain access to the bank account. (1½)
12. The passwords should only be valid and accepted by the system during business hours of the company. (1½)
13. Failed password login attempts should be logged and investigated. (1½)

(1½ for each valid point to the max. of 10 marks, available 18 marks)