Tutorial Letter 202/2/2018

INTERNAL AUDIT PROCESS: SPECIFIC ENGAGEMENTS AND REPORTING

AUI3703

SEMESTER 2

Department of Auditing

IMPORTANT INFORMATION

This tutorial letter contains important information about your module.

BAR CODE

Learn without limits.

UNISA university of south africa

CONTENTS

1 BRIEFING

This tutorial letter contains the solutions to Assignment 02 for this semester. The lecturer has marked a selection of the questions in this assignment. The marks you received for your answers to these questions will constitute your mark for this assignment and will contribute towards your year mark. You need to assess your answers to the other questions yourself by comparing your answers to those provided in this tutorial letter.

Use the marking plan as a guide to award yourself marks for your answers. Take care not to mark the same concept more than once just because it appears more than once, perhaps in different words or in a different format.

After you have marked your own answers, please reflect carefully on your result to determine why you could not allocate full marks to your answers. Please ensure that you allocate marks only to valid answers. It is imperative that you identify your problem areas now, while you can still do something about them. If you do not solve all your problems as soon as you have identified them, you may repeat the same mistakes in the examination, and that could prove very costly. Marking your answers should enable you to identify any problems you may be experiencing. Your marks for this assignment will be an indication of your level of knowledge of the module content at this stage. You should still have enough time left to revise the work and solve the identified problem areas before the examination.

We trust that you have found the assignment both interesting and informative and that it has served as an aid for your examination preparation. Should you encounter any difficulties regarding this module in internal auditing, please do not hesitate to contact us.

Lecturer

AUI3703

2 KEY TO ASSIGNMENT 02/2018 (2ND SEMESTER)

QUESTION 1 **33 marks**

1.1

General Controls are those controls which:

- establish an overall framework of control (1) over computer activities and which
- should be in place before any processing of transactions gets underway i.e. independent of processing. (1) For example, an appropriate organisation structure should be in place as well as sound access controls.

Application controls are controls over:

- input, processing and output of financial information relating to a specific application (1) e.g. wages to ensure that
- such information is valid (have occurred and are authorised), accurate and complete e.g. the authorisation of a purchase order (1). They are controls which are relevant to a task within a specific application. (1)

(Maximum 5 marks)

1.2.1 Control environment – *management philosophy and management style*

Weakness 1. Zak Kruger, to whom Dion Reddy reports does not get involved in any aspect of the company's computing, including very important matters such as the creation of user profiles.

Explanation 1. Zak Kruger as the financial manager should provide leadership and engender control awareness in his staff; as he doesn't get involved Dion Reddy can do precisely what he likes e.g. allocate user privileges.

Weakness 2. Zak Kruger and the other managers promote a relaxed and casual atmosphere at the company.

Explanation 2. Providing access to all employees to computer games and the internet, and allowing unnecessary socializing in the Techno Room may be enjoyable but is unlikely to promote sound and efficient controls. Whilst it is positive that employees enjoy coming to work, a casual atmosphere usually leads to a casual approach to controls and "exploitation" of the company e.g. abuse of access privileges, failure to meet internal control objectives, and a lack of control awareness.

Control Environment - *Organisational structure, assignment of authority and responsibility*

Weakness 1. There is no IT steering committee (see also pt 3).

Explanation 1. This firstly means that the IT section (a very important section) has no direct representation on the Board to give it authority and to assist in promoting a strong control environment.

Secondly, the absence of a strong steering committee increases the risk that poor, inappropriate decisions pertaining to computer matters will be taken and that inadequate control over the section will be exercised.

Thirdly, because there is no steering committee, Dion Reddy reports to the financial manager who, in effect, has little relevant knowledge or authority.

Weakness 2. Dion Reddy is given too much authority in respect of computer matters and fulfils functions which should be carried out by others.

Explanation 2. Dion Reddy's "sole responsibility" for employing computer staff, and purchasing computer equipment may result in unsuitable staff being employed and money being wasted on substandard or unnecessary equipment.

(Note, Dion Reddy should have a say in who is appointed and what is purchased, but not sole responsibility.)

Control environment – *participation of those charged with governance*

Weakness 1. The financial director does not get involved in the IT side of the business.

Explanation 1. IT governance, even in medium sized enterprises, is the responsibility of the board and it should provide the required leadership. There should be a channel of communication and regular reporting by IT (Dion Reddy) to the board.
The IT section at Rexon (Pty) Ltd is only answerable to itself.

Control environment – *human resource policies and practices*

Weakness 1. Rexon (Pty) Ltd has failed to implement certain important human resource practices.
proper recruiting policies are not in place.
passwords are not changed when an employee leaves.

Explanation 1. (i) Although Dion Reddy and his staff are technically very knowledgeable, they (or at least Dion Reddy) should have a working knowledge of accounting systems and related internal controls. Their lack of knowledge (and the lack of managerial support) has contributed to poor basic internal controls e.g. inadequate division of duties, poor access controls. Had proper background checks been carried out, this lack of competence would have been identified.
(ii) Not invalidating personal passwords when an employee leaves, increases the risk of unauthorized access by the former employee. This compromises the integrity of the system particularly where the employee has been dismissed. The problem with recruitment is compounded by the fact that Dion Reddy (as mentioned) is solely responsible for the recruitment of computer personnel.

(Maximum 8 marks)

1.2.2. Access Controls

Weakness 1 With regard to the company's security policy, it would appear that at least one of the basic requirements of a good security policy is not followed, i.e. the least privilege policy. All employees are given access to the computer system even though they do not require it to fulfil their functions e.g. pickers and packers.

Explanation 1 By providing legitimate access capabilities to all staff, the chance of compromising the integrity of the company's system is significantly increased e.g. hacking, destruction of data, damage to equipment.

Weakness 2 Access to all applications is available through any terminal. Terminal identification/profile controls are inadequate.

Explanation 2 By failing to restrict the applications (and modules within applications) to which a specific terminal can gain access, basic division of duties is compromised and the risk of unauthorized access to a specific application is increased.

Whilst access to applications and modules is restricted (potentially), enhanced access control could be achieved by setting up the network in a way which for example, does not allow access to the payroll application other than through specific terminals in the accounting department.

Weakness 3 Personal passwords are:
too simple and easy to work out.
not changed regularly enough.
passed on to the replacement employee when an employee leaves.
not kept private.

Explanation 3 (i) Even though the password is six digits, the first three will be known to all employees as they indicate the department the employee works in. In effect the password becomes a very simple numeric sequence of three digits.
(ii) Having unchanged simple passwords means that within a very short time all passwords will be known and will be totally ineffective as an access control.
(iii) by not withdrawing passwords, former employees, who may have malicious intentions, will still be able to access the company's systems without much difficulty.
(iv) having personal passwords authorised by the computer section again compromises the basic requirement that passwords remain private.

Weakness 4 (i) Employees themselves are able to change their access privileges.
(ii) Dion Reddy can change user profiles as he wishes.

Explanation 4 The user profile defines what the user has access to and is therefore a fundamental internal control in respect of confidentiality and division of duties. Allowing employees to decide what access they should have negates these controls. User profiles should be designed by people with a thorough knowledge of internal controls and all changes should be authorised at the highest level and controls should be in place to ensure that no unauthorised changes are made.

(Maximum 11 marks)

1.2.3. Continuity of operations

Weakness 1 The positioning of important components of the hardware e.g. servers, in a room with other general office equipment which is not access controlled and which is used as a staff gathering place where drinks are available compromises continuity of operations.

Explanation 1 (i) These conditions increase the risk of unintentional damage to the hardware e.g. coffee or tea could be spilled on a printer resulting in its malfunction.

(ii) The failure to physically secure (access control) the hardware increases the risk of intentional damage to the servers (sabotage), hacking and theft.

Weakness 2 Granting access to all employees i.e. failure to implement the least privilege principle.

Explanation 2. Allowing 80 employees (logical) access, (a number of whom have no need to have access), and particularly to the Internet, substantially increases the risk of unauthorized entry to the system, virus contamination, data destruction and hardware damage resulting in disruption of the system.

Weakness 3 Data is inadequately backed up:

* no automatic back up as a first line of defence
* not taken frequently enough and
* the external hard drives are inappropriately stored.

Explanation 3 (i) The company appears to not make use of software which automatically backs up data and stores it on an (independent) server.

(ii) Backing up every two months means that a great deal of information (including month-end information) could be lost should a disaster occur.

(iii) Simply locking the external hard drives in a (non-fire proof) desk at the office as opposed to storing them off-site does not sufficiently protect the company against the risk of losing the data should a disaster occur e.g. fire at the premises or theft.

Weakness 4 There appears to be no ongoing risk assessment process pertaining to IT.

Explanation 4 With no steering committee, no leadership or intervention from the board or Zak Kruger and no obvious attempt to address the numerous weaknesses in the company's IT, risks are neither being identified nor responded to. This will ultimately lead to negative consequences which will affect the continuity of operations, e.g. fraud, destruction of equipment, virus attack, etc.

(Maximum 9 marks)

QUESTION 2 **10 marks**

2.1

Statement of condition:

A customer refused to sign a delivery note that included items that were never ordered by them. They did, however, accept delivery of the goods they did order and noted them on a sheet of paper signed by their goods received clerk. (1)

Criteria:

Deliveries to customers should be accompanied by delivery notes and invoice. Upon delivery of the goods to a customer, the customer must sign the delivery note to acknowledge receipt of goods and retain the invoice. The delivery note is to be sent back to sales. (1)

Cause Dispatch failed to ensure that the goods delivered were the actual goods ordered by comparing the delivery note and invoice to the order documents and the actual goods delivered. (1)

Effect Customers could be invoiced inaccurately. This could result in a bad reputation for the company. Goods may be lost, stolen or unaccounted for resulting in financial losses. (1)

Recommendation A copy of the order documents should be sent to dispatch and the dispatch clerk should verify that the goods packed onto the delivery vehicle are the goods as per the order document and the delivery note and invoice. (1)

(Marks as indicated. Max 5 marks)

2.2 Briefly describe what a well-designed final communication should include.

- Purpose and scope of engagement (½)
- Time frame covered by the engagement (½)
- Observations as required by the evaluation and escalation process (½)
- Engagement conclusion and rating (½)
- Management's action plan to appropriately address reported observations. (½)
- If the report is longer than 4 pages then an executive summary is necessary (1)
- Findings should be rated with higher rated findings occurring in the front of the report while other less important findings in an appendix (1)

(Marks as indicated. Max 5 marks)

QUESTION 3 (24 marks)

3.1 List warning signs and internal control weaknesses given in the information that could have aroused suspicion that the ordering, sales, production and dispatch staff could be engaging in fraudulent activities and other white collar crimes.

Warning sign	Recommendation
Incorrect dispatching of goods is a way of bypassing controls.	The dispatch clerk should compare goods dispatched to the approved order and delivery invoice. Goods not on the invoice should not leave the premises.
Customers operating from the same premises could be a sign of them being suspicious.	New customers should be vetted before the company does business with them.
Unauthorised trips could be trips to deliver goods stolen from the company.	The company should get a tracking system that records trips taken. A report from the system should be monitored weekly.
Tyres have a useful life. When they are changed before that period has expired that should have raised suspicion.	The delivery vans should be thoroughly inspected by the dispatch manager before they leave the premises and when they return.

High fuel expenditure is a sign of theft of the fuel.	The company should have fuel cards and the drivers should be instructed to keep receipts for every filing they make. They should also be instructed to keep a log of their deliveries. The receipts should be compared to the logs.
Lack of segregation of duties between goods receiving and supplier payments.	There should be segregation of duties between goods ordering, goods receipts, goods keeping and supplier payment.
The expensive things and cars that some of the staff members have raised suspicion.	Fraud investigations should be conducted around the processes conducted by the staff members that display inexplicable wealth.
Lack of segregation of duties between income accounting and customer information management.	There should be segregation of duties between expenditure accounting and customer information management.
Disappearance of payment documents could be attempts to destroy the audit trail.	The person that performs the last task when processing the payments should have the sole responsibility to file the payment documents.
There are poor security measures to guard against theft of goods.	The company should consider having a security guard to inspect cars that are leaving the premises for unauthorised departure with goods.

(1 mark for each warning sign listed and 1 mark for each valid recommendation. Maximum of 20 marks.)

3.2 Name the elements of fraud

- Misrepresentation
- Cause prejudice
- Unlawful
- Intentional

(One mark for each principle listed. Maximum of 4 marks.)

QUESTION 4: (22 marks)

4.1 For each of the statements indicate whether it relates to effectiveness, efficiency or economy and formulate an audit procedure.

Number	Efficiency, economy, effectiveness	Audit procedure
i	Efficiency (1)	Trace the various orders from the different sources through the various departments and determine whether the orders are forwarded timeously and that telephone orders are taken in a manner that is understandable and readable. (1½)
ii	Efficiency (1)	Trace the various orders sent to sales to determine the timeframe within which they are processed to establish if there are any delays. (1½)
iii	Effectiveness (1)	Inspect a sample of processed orders to determine if they were all approved. (1½)
iv	Efficiency (1)	Enquire from management who from sales department is responsible for receiving orders from the receptionist for processing and inspect a sample of orders to verify that they are received by that person. (1½)
v	Effectiveness (1)	Enquire from management why the invoices are sent out before the orders have been fulfilled. (1½)
vi	Efficiency (1)	Enquire from management how the daily production relates to the orders to be fulfilled. (1½)
vii	Economy (1)	Enquire from management as to whether the pricing done at production is inclusive of other overhead expenses. (1½)
viii	Economy (1)	Through observation of the warehouse facility, check to see that the warehouse space is used fully and that there are no major empty spaces. (1½)
Ix	Economy (1)	Compare the price of leasing the machinery to the price of purchasing it. (1½)
x	Efficiency (1)	Enquire from management how the receptionist decides on the quantities to be ordered. (1½)

xi	Economy (1)	Enquire from management whether competitive bidding was done when deciding on the supplier. (1½)
Xii	Economy (1)	Enquire from management how the dispatch staff work schedules are matched to the deliveries to be made. (1½)
Xiii	Effectiveness (1)	Through observation, determine how quality control is performed at the end of production. (1½)

(Marks as indicated. Maximum 22 marks.)

---©---

UNISA 2018