AUE2602
SUGGESTED SOLUTION EXAM MAY / JUNE 2013

QUESTION 1 **50 MARKS**

1.1 The requirements of sound corporate governance pertaining to the board of directors and board committees **25 marks**

Reference: The King III Report (2009:29-75)

1. Board of directors: composition and appointments

1. M Lebete, the chairman of the board, is **not** an independent non-executive director (Principle 2.16). (1½)
2. S Gouws, the chief executive officer (CEO), is not the chairman of the board, which is in **accordance** with the Principle 2.16. (1½)
3. The board should comprise a balance of power with a majority of non-executive directors who should be independent. The board has only one independent non-executive director and does **not** comply with principle 2.18. (1½)
4. At least a chief executive director and finance director should be appointed to the board (Principle 2.18, point 73). Minetech does **not** currently have a financial director acting on the board (for the past six months). (1½)
5. Appointments to the board should be a matter for the board as a whole, assisted by the nominations committee (principle 2.19, point 80), and **not** the CEO, S Gouws, alone (financial director appointment). (1½)

Limited to 4 valid answers

2.Board of directors: meetings

1. Non-executive directors should ensure that they have the time required to attend properly to their duties (principle 2.19, point 83). L Pretorius, the independent non-executive director, does **not** meet this requirement. (1½)
2. Minetech's board meets only twice a year, and **not** 4 times a year as required by principle 2.1 point 1. (1½)

Limited to 2 valid answers

3. Audit committee: composition and appointments

1. All members should be independent non-executive directors (Principle 3.2 point

9). Minetech does **not** comply as only L Pretorius is an independent non-executive director. (1½)

2. The audit committee is not independent if two thirds of membership, which includes the chairman (influential), are **not** independent non-executive directors (Principle 3.2). (1½)
3. Minetech **complies** with principle 3.2 point 10 with its minimum of three members. (1½)
4. Audit committee members should be suitably skilled and experienced (Principle 3.2 and point 12). Minetech does **comply** with this requirement as L Pretorius is a CA(SA) and A Peters an IT specialist who knows computerised accounting systems well. (1½)

Limited to 3 valid answers

4.Audit committee: meetings

1. Minetech **complies** with principle 3.1 point 7's requirements to meet at least twice a year. (1½)
2. Minetech **complies** with principle 3.1 point 8's requirements to meet with internal audit at least once a year. (1½)
3. Minetech does **not** comply with principle 3.1 point 8's requirements to meet with internal and external audit at least once a year. (1½)
4. Minetech does **not** comply with principle 3.1 point 8's requirements to meet with internal and external audit without management being present (with reference to M Lebete and A Peters who are also part of management). (1½)

Limited to 3 valid answers

5. Risk committee: composition and appointments

1. The chairman, M Lebete, should not chair the risk committee but may be a member of it (Principle 2.16, point 45.4). Minetech does **not** comply with this requirement as M Lebete is also the chairman of the risk committee. (1½)
2. The risk committee has only two members and does **not** comply with the requirements of principle 4.3 point 21 of three members. (1½)
3. The risk committee has executive and non-executive directors as members, which **complies** with principle 4.3 point 20. (1½)
4. Principle 4.3 point 20 requires members of the risk committee to have, as a

whole, adequate risks management skills and experience. H Ally, the risk director, should have the necessary skills and experience and **complies** with the principle. (1½)

Limited to 2 valid answers

6. General remarks

1. The board has a company secretary in **accordance** with principle 2.21 point 95. (1½)
2. The board should appoint audit-, risk-, remuneration- and nomination committees (Principle 2.23, point 129-130). Minetech does **not** have remuneration and nomination committees. (1½)
3. Risk is an ever present factor in any large company, and risks change. It is unrealistic for Minetech Ltd to think otherwise and the theft committed by the financial director is an example of a current financial threat faced by the company. Mineco did **not** comply with principles of good governance of risk (principle 4.1) (1½)
4. Overall, the board of directors and board committees do **not** meet the King III Report's requirements for good corporate governance. (1½)

Limited to 2 valid answers

7. Presentation

Presentation of answer under sub-headings provided in paper. (2)

(1½ for each valid point compliance or non-compliance to the max. of 25 marks, available 36 marks)

Comments to markers:

- **Students are required to comment on both compliance and non-compliance.**
- **Students only have to identify compliance / non-compliance with brief explanations; and not also the King III principle or requirement. The memorandum includes these for reference purposes.**

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)

QUESTION 2 **50 MARKS**

2.1 Internal controls over the ordering of goods in a manual system 15 marks

Reference: - Jackson & Stent (2010: 11/9)

Risk 1

1. Order clerks should not place an order without receiving an authorised requisition. (1½)
2. The order should be cross referenced to the requisition. (1½)
3. Prior to the requisition being made out, stores/production personnel should confirm that the goods are really needed. (1½)

Risk 2

1. Before the order is placed, a supervisor/senior buyer should:
    - check the order to the requisition for accuracy and authority; (1½)
    - review the order for suitability of supplier, reasonableness of price and quantity, and nature of goods being ordered. (1½)
2. Segregation of duties should exist between the ordering and authorisation duties. (1½)

Risk 3

1. The company should preferably have an approved supplier list to which the buyer should refer when ordering. (1½)

Risk 4

1. Before a supplier is approved, senior personnel should carefully evaluate the pricing of products of the company. (1½)
2. The suppliers masterfile could include a price list of goods normally/contracted to be purchased from the supplier. (1½)
3. If goods need to be purchased from a supplier other than the usual approved suppliers, or goods not included in the above price list, a quotation should be obtained for goods to be ordered. (1½)

Risk 5

1. Before a supplier is approved, senior personnel should carefully evaluate the reputation of the supplier with regards to reliability. (1½)

2. Even when ordering from an approved supplier, the buyer should contact the supplier to confirm availability and delivery dates. (1½)
3. The ordering department should file requisitions sequentially by department and should frequently review the files for requisitions which have not been cross referenced to an order. (*purchase requisitions cross referenced to purchase orders*) (1½).
4. A copy of the order should be filed sequentially. (1½)
5. The file should be sequenced checked and frequently cross referenced to goods received notes, to confirm that goods ordered have been received. (*copies of orders cross referenced to goods received notes*)(1½)
6. Alternatively the pending file of purchase order forms in the receiving bay can be reviewed for orders which are long outstanding. (1½)

Risk 6

1. Blank order forms should be subject to sound stationery controls. (1½)

(1½ for each valid internal control to the max. of 15 marks, available 18 marks)

2.2. Application controls over the suppliers (creditors) masterfile in a computerised environment 15 marks

Reference: - Jackson & Stent (2012: 11/17 – 11/18)

1. All amendments to be recorded on hardcopy masterfile amendment forms (MAFs). (1½)
2. MAFs to be pre-printed, sequenced and designed in terms of sound document design principles. (1½)
3. The MAFs should be signed by two senior personnel after they have agreed the details of the amendment to the supporting documentation. (1½)
4. Restrict write access to the creditors masterfile to a specific member of the section by the use of user ID and passwords. (1½)
5. All masterfile amendments should be automatically logged by the computer on sequenced logs and there should be no write access to the logs. (1½)
6. To enhance the accuracy and completeness of the keying in of masterfile amendments and to detect invalid conditions, screen aids and programme checks can be implemented:

screen aids and related features:

- Minimum keying in of information. (1½)
- Screen formatting, screen looks like MAF, screen dialogue. (1½)
- The account number for a new supplier should be generated by the system. (1½)

programme checks:

- Verification/matching checks to validate a creditors account number against the creditors masterfile. (1½)
- Alpha numeric checks. (1½)
- Data approval check(1½) (for example they must enter either 30 days or 60 days in the payment terms field, not say, 120 days)
- Mandatory/missing data checks (1½) (for example credit limit and terms must be entered)
- Sequence check on MAFs entered. (1½)

7. The logs should be reviewed regularly by a senior staff member and the sequence of the logs themselves should be checked for any missing logs. (1½)
8. Each logged amendment should be checked to confirm that it is supported by a properly authorised MAF and that the details are correct (1½).
9. The MAFs themselves should be sequence checked against the log to confirm that all MAFs were entered(1½).

(1½ for each valid control to the max. of 15 marks, available 24 marks)

2.3 Procedures to follow when conducting an physical year-end inventory count 20 marks

Reference: - Jackson & Stent (2012: 12/12-12/13)

1. The count staff should be divided into teams of two, with one member of the team being completely independent of all aspects of inventory. (1½)
2. All teams should be given a floor plan of the warehouse which should clearly demarcate the inventory locations for which they are to be held accountable. (1½)
3. All inventory should be counted twice. One of the following methods can be adopted:
   - One member of a team counts and the other records, swapping roles thereafter and performing a second count in the same section to which

they were assigned. (1½)

- Count teams complete their first counts, hand their inventory sheets back to the count controller and sign for the inventory sheets of another section, thereby doing their second counts on a section already counted by another count team. (1½)

4. As items are counted they should be neatly marked by the counters. (1½)
5. Where count teams identify damaged inventory these inventory items must be marked as such on the inventory sheets. (1½)
6. The contents of boxes where the packaging appears to have been tampered with, should be counted and the details noted on the inventory sheet. (1½)
7. A few boxes should be selected at random in each section and the contents compared with the description on the label to confirm that the contents have not been changed/removed and the seal replaced. (1½)
8. The count controller (and assistants) should:
   - walk through the warehouse once the count is complete and make sure all items have been marked twice. (1½)
   - examine the inventory sheets to make sure that first and second counts are the same and agree to the quantities recorded on the perpetual inventory system if there is one. (1½)
   - instruct the count teams responsible for sections where discrepancies are identified to recount the inventory items in question. (1½)
9. The count controller should obtain the numbers of the last goods received note, invoice, delivery note and goods returned note used up to the date of the inventory count. (1½)
10. No despatches of inventory should take place on the date of the inventory count. (1½)
11. Any inventory received after the count has begun should be stored separately in the receiving bay, until the count is complete and must not be put into the stores. This inventory must be counted and added to the inventory sheets after the count is complete. (1½)
    - The counters responsible for the count sheets should draw lines through the blank spaces on all inventory sheets, and sign each count sheet and all alterations. (1½)
12. The inventory controller should check that this procedure has been carried out(1½) and should sequence test the inventory sheets to ensure that all sheets

are accounted for. (1½) 13. Count teams will only be <u>formally dismissed</u> once the count is complete and all queries have been attended to. (1½) **(1½ for each valid count procedure to the max. of 20 marks, available 27 marks)**					