STRICTLY CONFIDENTIAL

THE PUBLIC ACCOUNTANTS EXAMINATION COUNCIL OF MALAWI

2013 EXAMINATIONS

ACCOUNTING TECHNICIAN PROGRAMME

PAPER TC 4: INFORMATION SYSTEMS

WEDNESDAY 4 DECEMBER 2013 **TIME ALLOWED: 3 HOURS**
2.00 PM - 5.00 PM

SUGGESTED SOLUTIONS

1. (a) Application served:

- Transaction processing system
  - payroll, inventory production, sales, accounting.
  - management information system.
  - production control, sales forecasting, monitoring.
- Decision support system
  - long range strategic planning, complex integrated problem areas.
- Expert system
  - diagnosis, strategic planning, internal control planning, maintenance strategies.

(b) Database facilities

- Transaction processing systems.
- Unique to each transaction, batch update, online updates.
- Management information system.
- Interactive access by programmers.
- Decision support system
  - database management system.
  - interactive access, factual knowledge.
- Expert system
  - procedural and factual knowledge, knowledge base.

(c) Decision capabilities:

- Transaction processing system:
  - no decision or simple decision models.
- Management information system
  - structured routine problems using conventional operations research tools.
- Decision support system:
  - semi-structured problems, integrated on models, blend of a judgment and structured support capabilities.
- Expert system:
  - the system makes complex decisions, unstructured, use of rules.

(d) Type of information output

- Transaction processing systems:
  - summary reports, operational reports
- Management information systems
  - Schedules and demand reports, structured flow, exception reporting.
- Decision support system:
  - information to support specific decisions.
- Expert system:
  - advice and explanations.

(e) Level served within organization

- Transaction processing system:
  - operational staff, low management.
- Management information systems:
  - middle management.
- Decision support systems
  - top management
- Expert system
  - top management, specialists.
  -

2. (a) First generation computers 1940 – 1956

- used vacuum tubes for circuitry
- magnetic drum for memory
- were very enormous
- expensive to operate and using a great deal of electricity
- generated a lot of heat
- relied on machine language to perform operations
- could only solve one problem at a time
- input was based on punched cards, paper tape
- output was displayed on printouts
- examples were the UNIVAC and ENIAC.

(b) Second generation computers 1956 – 1963

- transistors replaced vacuum tubes
- this allowed computers to become smaller and cheaper
- they became more energy efficient
- they still relied on punched card
- output still on print outs
- used assembly language for specific machines and processors
- could still solve one problem at a time
- high level programming languages were being developed
- they stored their instructions in memory
- moved from a magnetic drum to magnetic core technology
- they were developed for the atomic industry.

(c) Third generation computers 1964 – 1971

- the development of the integrated circuit (IC)
- transistors were placed on silicon chips called semiconductors
- many applications could run at one time
- a central program controlled the memory
- keyboard replaced punched cards
- monitors were developed that added the output to printouts
- users interfaced with operating system through the keyboard and monitors
- COBOL and BASIC were fully operational
- other high level computer languages were being developed
- languages were multi-user not machine or memory specific
-
- price drastically reduced as the computer would solve a lot of application tasks.

(d) Fourth generation computers – 1971 –

- the microprocessors were developed
- thousands of integrated circuits were built on to a single silicon chip
- the computers could fit in the palm of the hand
- the intel 4004 chip was developed
- located all the components of the computer from the control processing unit and memory to input/output controls on a single chip

- fourth generation computer languages were developed
- computer could be linked to one another
- internet was developed
- they saw development of graphic user interface (GUI), the mouse, and handheld devices
- computers were used in security processes (biometrics)
- use of wireless devices in computer (bluetooth) etc.

3. (a) "Top down" system development is a general concept rather than a particular methodology. As the name suggests, this approach initially considers management strategic needs and goals prior to specifying operational data requirements. The higher level functions are then progressively analyzed into more detail. In protease, there can exist a degree of interaction in the approach as the review of the impact of lower level situations or operational needs on the higher level functions can indicate whether it is necessary to revise the higher level goals. The top down approach requires a high degree of top management involvement in the planning process and focuses on organizational goals, objectives and strategies.

"Bottom up" is the process of designing the system which starts with identifying the process that need computerization as they arise, analyzing them as systems and either coding or purchasing packaged software to meet the immediate problem requirement. The applications which benefit from the computerization will most frequently be found at lowest level of the organization. Business often take this approach to systems development by the external acquisition of, for example, software packages for accounting, a different package for production scheduling and another for marketing and so on. Although each subsystem appears to get what it wants, when overall system is considered, there are severe limitations taking a bottom-up approach. It is a pro-active approach.

(b) (i) Advantages of top down systems development:
- lends itself to prototyping
- easy to integrate and interface applications and routines
- project teams are able to interface their designs more satisfactorily.
- ensures that the creation of a comprehensive data base which aids flexibility in response to new requirements.
- encourages a structured (modular) approach to systems design.

(ii) Advantages of bottom-up:

- Problems for which computerization is cost effective are addressed first.
- Staff morale is improved as staff are fully involved.

(c) (i) Disadvantages of top down:

- Difficult to apportion the system so that it makes sense for the total system picture
- Once subsystem divisions are made, their interfaces may be neglected or ignored (responsibility for interfaces need to be detailed) because subsystems must be re-integrated eventually.
- Security may be compromised between subsystems.

(ii) Disadvantages of bottom-up:

- Duplication of data and data entry
- Worthless data may be entered into the system
- Duplication of effort in purchasing software
- Difficult to interface the subsystems so that they perform smoothly as a system
- Excessive detail means that the analyst loses sight of what the system is supposed to do.
-

4. (a) Anybody or an organization offering any service related to computing, either as a main line of business or a sideline can be considered as a computer bureau.

(b) Seven major functions of a computer bureau are:

(i) To provide hardware on clients premises either on rental, or lease or purchase for clients.

(ii) To provide hardware to its clients where data is taken to the bureau for processing and results returned.

(iii) Software provision, the bureau writes application software to various organizations that request it.

(iv) Consultancy: provides advice on buying and installing in house computer systems.

(v) Security: bureaus offer off-site storage facility.

(vi) Security: bureaus provide secure data transmission channels.

(vii) Provision of software: clients go to the bureau to use some once off software or the bureau's software for a specific purpose e.g. conversions of files.

(viii) Provides computer staff: trains the staff in punching, operating etc.

(ix) Courier services: clients go to the bureau for movement of computer related items.

(c) Guidelines to follow when selecting a computer bureau are:

- identify what jobs you have for the bureau.
- outline frequency that you would require the bureau and if possible without a time estimate for doing them.
- prepare a benchmark job and approach several reputable bureaus or use a broker to obtain quotations.
- you need to ascertain the availability of hardware and its compatibility with your system.
- ascertain availability of adequate operating systems and software compatibility.
- experience, reliability, reputation and the bureaus financial stability.
- real service provided and extras.
- if they can handle your specific requirement.
- confidentiality, security and insurance arrangements with the bureau.
- delivery dates and turnaround time.
- appoint a bureau liaison officer who will negotiate contracts and prices.

5. (a) (i) A computer language is a language that is used by computer programmers to pass instructions (communicate) to the computer (machine); in other words, a computer language is a language that computer programmers use to talk, communicate or instruct the computer. Just like there are many languages human use to communicate so are computer languages.

(ii) (1) A low level computer language can be described as a language that is in machine code or assembly code. It is usually embedded in computer chips. This is mostly in pure binary e.g.

Function	Address
101	1011

It is difficult to learn and understand.

(2) The law level computer languages are used for computer oriented problem and are mainly hardware oriented. Such are programs that run to check hardware during boot up as an example. They cannot be modified by the computer user.

(iii) Examples of low level language are: machine code, assembly language.

(iv) (1) A high level computer language is a language which is structured to accept statements with English like structures. These languages require a compiler in order for the machine to understand the instruction being passed on.

(2) These languages are usually used when solving a functional problem i.e. an application problem. They are developed to be used in solving numerous application problems otherwise are used when developing application software.

(v) Examples of high level computer languages include cobol, basic, 4GL, pascal etc.

(b) (i) A computer compiler is a program that is written to accept a source program in a high level language and converts it to a particular machine code program that would be understood by the computer to perform a particular task as required by the high level source.

(ii) A computer compiler is required in a business organization because it enables the organization to customize the source codes of their application software to suit the organization's changing needs by just a change in the source code and a compilation to get the result. Most 4^{th} generation languages have built in compilers as such that during or after changing the source program, a compiler is invoked.

6. (a) (i) Memory: This enables a computer to store, at least temporarily data and programs that are being executed.

(ii) Mass storage device: Allows a computer to permanently retain large amounts of data. Common devices include disk drives and tape drives.

(iii) Output device: This is a device that shows you what the computer has accomplished – information. Common examples are: printer, monitor (VDU).

(iv) Input device: This is a conduct through which data and instructions enter a computer. Examples are – keyboard and mouse – touch pad etc.

(v) Central processing unit(CPU): This is the heart of the computer. This is the component that executes instructions.

(vi) Bus – bus is required to transmit data from one part of the computer to another.

(b) Firewall

Common firewalls protect against the spread of fire or other danger. By extension, the computer firewall is a term used for a piece of hardware or software which functions in a networked environment to prevent some communications forbidden by the network policy. It has the basic task of preventing intrusion from a connected network device into other networked devices. Prevents hackers from unauthorized access.

7. (a) Physical control of computer hardware:

(i) Computer room must be locked to avoid theft of equipment.

(ii) Access to computer room be restricted to authorized staff only through door password to avoid malicious damages.

(iii) Fire extinguishers be installed in the computer building in readiness for a fire outbreak.

(iv) All visitors to computer room must sign a log book so that they are traceable in case of an eventuality.

(v) Computer room be placed on a high ground to guard against flooding.

(vi) A UPS be installed to guard against hardware failure due to power outage.

(vii) All hardware specifications for use to be followed to avoid malfunctions.

(viii) All hardware be identified in an asset register in order to trace its movements.

(b) (i) Use of access passwords for data and programs to avoid fraud.

(ii) Rotating staff to avoid tricks.

(iii) Use of register for reports to avoid loss of reports.

(iv) Use of computer generated numbers for important documents such as invoices to secure against illegal documents.

(v) Attend to all exceptional reports to ensure accuracy in the system.

(vi) Regularly backup data to avoid loss of data in case of a disaster.

(vii) All updates to important master files be logged to avoid illegal updates.

(viii) Discard all used reports carefully to avoid leakage of information through this process.

(ix) Use of firewall when on a network to avoid hackers.

(x) Use of an up-to-date antivirus software to avoid viruses attack on the system.

(c) Control of consumables

- follow manufacturers specifications as regards storage and handling to avoid malfunction.
- register all movements to avoid loss.
- physical check on staff to avoid theft.
- discard all consumables following manufacturers recommendation to avoid leakage.
- restrict use of such consumables as disks from outside organization to avoid information theft.
- restrict all hardware consumable that may contain viruses to be used on the computers to avoid virus attack.
- password protect all wireless gadgets to avoid illegal access.

8. (a) Tangible costs:

- Capital cost items
  - hardware purchase costs
- Working capital (supplies of paper, disks etc)
  - once-off revenue cost items
  - consultancy fees (if any)
  - systems analyst and programmers' salaries

- cost of testing the system
- cost of converting the files for new system
- redundancy payments (if any)
- initial staff training.

- Regular annual costs
  - operating staff salaries/wages
  - data transmission costs
  - consumable material costs
  - power supply
  - extra rental costs
  - hardware maintenance costs
  - cost of software system support
  - cost of standby arrangements
  - regular staff training
  - equipment insurance costs

(b) Intangible costs include:

- staff morale problems
- repetitive strain injury
- other physical problem associated with use of computers
- the fact that computers can be inflexible
- computer systems can be expensive to modify
- problems arising from out of date data
- problems arising from accepting computer results as accurate.
- computer system can be expensive to replace.
- rapid technological charges and strain company resources.
- costs related to prevention of by-products such as viruses.
- cost arising from protecting yourselves against hackers.
- costs arising from illegal use of equipment on internet.
- Costs arising from staff through illegal e-mail usage.

E N D