FEEDBACK TUTORIAL LETTER

1st SEMESTER 2017

ASSIGNMENT 2

ACCOUNTING INFORMATION SYSTEMS

AIS822S
Dear Student

I hope you have received your first assignment back as well as the feedback tutorial letter for the first assignment. If you have not received these, please call your student support officer at COLL.

This tutorial letter is to give feedback on Assignment 2 of Accounting Information Systems. Assure yourself of all the correct answers and pay attention to the remarks of the marker-tutor. Feel free to call me if you need assistance.

Use the time that you have available up to the end of the semester to do revision and to prepare yourself for the examination.

Good Luck with the examinations!

Regards,

Mr/Mrs

Email:
ASSIGNMENT 2

Instruction: Please answer each question on a new, clean page.

Question 1

Gawaseb Ltd has recently introduced an in-house training policy that requires all graduate entrants to the finance department to work within the internal audit department for the first 6 months of their training contract. The chief internal auditor of Gawaseb Ltd has asked you to contribute to the induction pack for next intake of graduate students. Prepare an essay for inclusion in the graduate induction pack explaining the importance and relevance of internal controls to a company such as Gawaseb Ltd. In your essay, you must distinguish between the different types of internal controls AND provide a brief summary of the possible risks associated with the failure of such internal controls in a creditor-based expenditure cycle.

Suggested answer

General controls

General controls relate to all activities involving the company’s/organisations resources, assets and facilities (including accounting information systems resources).
They are designed to:

- ensure that a company’s/organisation’s control environment remains stable and secure,
- maintain the integrity of corporate functions/activities (including accounting information systems processing functions/activities) and associated systems and networks,
- preserve the ongoing reliable of the company’s/organisation’s control environment and enhance the effectiveness of application controls,
- maintain appropriate levels of physical security practices and environmental protection measures to minimise the possible risk of vandalism, theft and/or sabotage and
- ensure the adoption of appropriate disaster planning and recovery protocols to ensure continuity of systems, networks and processing procedures

In an accounting information systems context, general controls seek to ensure that:

- all appropriate data is correctly processed,
- all systems applications and network functions and processes are operated in accordance with to established schedules and protocols,
- all processing errors are identified, traced and resolved,
- appropriate recovery procedures are established for processing failures,
- data/information file backups are maintained and updated at periodic intervals,
- systems/network development and change control procedures are applied and
- all related human resources activities are monitored and reviewed

General controls are generally classified into the following categories:
• organisational controls,
• documentation controls,
• access controls, asset management controls,
• management practice controls and
• information systems controls

Organisational controls
Organisational controls usually exhibit either a preventative control focus and/or a detective control focus and comprise of all those controls that are either derived from and/or related to the structural composition of a company. They are inevitably political in nature and are invariably associated with the hierarchical nature of the company and the structural relationship between company personnel – their duties, their activities and their responsibilities. In a social context, such controls normally manifest themselves in the form of:

• a functional separation of management/administrative processes, procedures and protocols – a preventative control focus,
• a segregation of duties, activities and responsibilities between company/organisation personnel – also a preventative control focus and
• the independent monitoring/reviewing of processes, procedures and protocols – a detective control focus

The purpose of organisational controls is to establish organisational autonomy or more appropriately, function/activity independence, with the primary objective being to ensure ‘the complete separation of incompatible functions and activities’. As such organisational controls normally seek to ensure a separation between:

• procedures concerned with the authorisation of transactions,
• activities associated with the custody of assets/liabilities,
• processes connected to the recording of transactions and
• functions related to the controlling of assets/liabilities

While there can be little doubt that the principle activities of the company – and its associated (externally imposed) regulatory requirements and the internal management/organisational structure of the company/organisation – and its associated internal politics will clearly influence:

• ‘how’ such a separation of management/administrative processes and procedures is realised
• ‘how’ such a segregation of duties and/or activities is implemented

Yet, it is the composition and availability of resources within the company that will, perhaps more importantly, determine the balance between a preventative control focus and a detective control focus.

Documentation controls
Documentation controls are all those controls associated with managing the format and content of all corporate documentation utilised in processes and procedures connected to:

- the acquisition and recording of data and/or information,
- the storage of data and/or information and
- the distribution of data and/or information

Such data/information can be permanent in nature – for example, data/information related to:

- established policies and procedures,
- management hierarchy,
- responsibility structures,
- administrative procedures and/or
- operational protocols and/or transactional in nature – for example, data/information related to:
  - all source input documentation
  - all documentation related to processing procedures and
  - all output-based documentation

Documentation controls should ensure that all documentation is controlled, all documentation (including changes to existing documentation) is approved prior to use and all (details and examples of) approved documentation is properly secured within a documentation library.

In addition to the above permanent and/or transaction data/information related documentation, where information systems technologies are used extensively in transaction processing additional documentation controls would exist – for example,

- **system documentation** – including documentation related to:
  - systems management and development policies,
  - information technology operations procedures and policies and
  - security and disaster recovery procedures and policies
- **systems application documentation** – including documentation related to:
  - application procedures (systems flowcharts and narrative descriptions),
  - data format and file descriptions,
  - input/output documentation (format descriptions and details),
  - charts of accounts (relationship schedules) and
  - control and error correction policies and procedures
- **system program documentation** – including documentation related to:
  - program procedures (program flowcharts and narrative descriptions),
  - input/output documentation (format descriptions and details),
  - change procedure and policies,
  - program content and listings,
  - test procedures and policies and
  - error reporting policies and procedures
- **data documentation** – including documentation related to:
  - data elements/format descriptions,
  - data element relationships
- **operating documentation** – including documentation related to:
  - performance and management instructions,
  - setup policies and procedures,
o recovery and restart policies and procedures and
o report distribution lists and procedures
• user documentation – including documentation related to:
o data input/entry policies and procedures,
o input accuracy/completeness checks,
o reports formats and
o error correction policies and procedures

Access controls
Access controls exhibit a preventative control focus and are all those controls associated with ensuring
• the security of company/organisation assets and resources,
• the integrity of corporate/organisational operations and activities and
• the confidentiality of corporate data and/or information, and minimising the risk of:
  • unauthorised/undetected access, loss,
  • misappropriation and/or
  • improper modification, deletion and/or alteration

Asset management controls
Asset management controls are all those controls associated with ensuring:
• assets are properly managed, suitably controlled and appropriately valued,
• assets are properly recorded and appropriate control registers/records are maintained of all asset acquisitions, transfers and disposals,
• periodic reconciliations are undertaken to confirm asset values and corroborate asset balances and
• periodic reviews and assessments are undertaken to determine the on-going condition of and relative value of the assets

Asset management controls seek to minimise possible financial loss associated with:
• accidental loss/damage,
• deliberate impairment,
• larceny,
• incorrect valuation and/or
• bad management decision making, and are closely associated with access controls and their role in maintaining/protecting the security of assets (discussed later)

Management practice controls
Management practice controls are all those controls associated with minimising management related risks – risks that may arise from:
• inadequate and/or unsatisfactory management decision making,
• deficient and/or incompetent management practices and/or
• dishonest and/or fraudulent management activities

Management practice controls include not only of the general controls discussed so far – organisational controls, documentation controls, access controls, and of course asset management controls – but also
all controls associated with ‘the management, administration and development of application systems’, and all those controls associated with systems management and development, in particular:

- amendment/modification controls and
- development management controls

Information systems controls

Information systems controls are all those controls associated with:

- information technology management and
- information systems administration

Information technology management controls seek to ensure the protected custody of computer hardware and related peripheral equipment, and, the security and integrity of software programmes.

Information systems administration controls seek to ensure ‘the correct and appropriate processing of data and information’ through:

- the scheduling of data collection activities,
- the continuous monitoring of data processing activities and
- the management of data/information output activities

Application controls

Application controls – sometimes called transaction controls – are controls that relate to specific aspects of a company’s/organisation’s processes, procedures, resources, assets and/or facilities (including accounting information systems resources).

They are designed to;

- prevent and detect transaction processing errors,
- identify transaction processing discrepancies and
- correct transaction processing irregularities

In an accounting information systems context, application controls (or application specific controls) seek to ensure that

- only authorised transaction data appropriate to the specific systems is processed;
- all transaction processing is efficient, effective, appropriate, accurate and completed in accordance with established systems-specific procedures and protocols;
- ensure systems-specific transaction processing procedures and transaction processing programs are secure and ensure all systems-specific transactions processing errors are identified and corrected and accounting for when an error occurs

Application controls are generally classified into the following categories:

- input controls (for example, undertaking editing tests),
- process controls (for example, ensuring appropriate record counts) and
- output controls (for example, maintaining error catalogues/listings)
Input controls

Input controls are designed to ensure the validity, appropriateness and correctness of system/application-specific input data, for example,

- payroll input data (for example, hours worked, hourly pay rates) are processed by the payroll system;
- purchasing input data (for example, payment of invoices) are processed by the purchasing system and
- sales input data (for example, the issue of sales invoices) are processed by the sales system and would, for example, include the use of:
  - appropriateness checks (for example, data matching checks),
  - authorisation procedures checks,
  - conversion controls tests (for example, batch control totals and/or hash control totals),
  - record count checks,
  - error identification tests/checks,
  - error correction procedure checks and
  - completeness checks (for example, sequence totals and/or control totals)

In addition to the above, where input data is transmitted (from a source origin to a processing destination), additional supplementary input controls would normally be required and would, for example, include

- transmission tests (for example, echo checks and/or redundancy checks),
- security checks (for example, verification checks) and
- validation checks

Processing controls

Processing controls are designed to ensure that:

- only authorised system/application-specific input/transaction data are processed,
- all authorised transaction data are processed accurately, correctly and completely,
- all appropriate program files/system procedures are used in the processing of transaction data,
- all processing is validated and verified and
- an appropriate audit trail of all transaction processing is maintained

Such controls would, for example, include the use of:

- file maintenance checks,
- file labelling checks,
- verification checks,
- processing logic checks,
- limit checks,
- reasonableness checks,
- sequence checks,
- audit trail controls,
- control totals checks and
- data checks (for example, checks for duplicate data and/or missing data)
Output controls

Output controls are designed to ensure that:

- all output is validated, verified and authorised;
- all output is accurate, reliable and complete and
- all output is distributed to approved and authorised recipients

Such controls would, for example, include the use of:

- distribution controls,
- verification checks,
- reconciliation checks, review checks (for example, source data/document comparisons),
- reconciliation of totals

In addition to the above, where output data is transmitted (from a processing origin to a user destination), additional supplementary output controls would normally be required and would, for example, include:

- transmission tests,
- recipient identifier checks,
- redundancy checks,
- security checks and
- validation checks (for example, continuity checks)

Question 2

Describe the main types of audit a company may be subject to.

Suggested answer

Types of financial statement audit

A financial statement audit (also referred to as a year-end audit (somewhat misleadingly) and/or a statutory audit and/or financial audit) is an examination (by an external auditor) of the records and reports of a company and an examination/assessment (by an external auditor) of the degree as to which a company’s financial statements are in accordance with generally accepted accounting principles and practices.

A financial statement audit can – if so required – be further divided into:

- a balance sheet audit,
- an income statement audit and
- a cash flow statement audit

The key features of a financial statement audit are:

- they are financial orientated,
- they are principally concerned with historical/static created representations and
they are orientated to/design for external corporate stakeholders and, as such are designed to substantiate/validate/verify and/or confirm the information contained with a company’s financial statements and facilitate the formulation of an opinion on whether the financial statements of a company provide a true and fair view of the company’s state of affairs as at the end of the financial year and its profit and loss accounting for the year.

Types of compliance audit

Internal control/systems audit

Mainly systems based, an internal control audit is an objective examination and evaluation of the effectiveness of a company’s internal control procedures in the prevention and detection of potential security threats and/or other financially damaging events/occurrences. Such an audit would also seek to assess the adequacy of management feedback processes and procedures in identifying and eliminating potential threats and risks to the company’s governance, present well-being and future survival.

An internal control audit is essentially an objective assurance/review process designed to:

- identify system requirements, procedures, processes and protocols,
- determine current compliance with existing system requirements, procedures, processes and protocols, determine areas of potential internal control weakness,
- provide a quantifiable risk assessment of any such internal control weaknesses and
- recommend possible improvement to internal controls to eliminate possible financial/nonfinancial loss, and as a consequence not only improve but also add value to the company’s activities and operations

Undertaken as part of a company’s on-going internal audit function, such an internal control audit would

- be mainly system based and
- aim to support the work of the company’s external auditor

Management audit

A management audit is an evaluation of performance and compliance in relation to regulatory, process, economic and efficiency-based accountability measures at all management levels. Such an audit focuses on outputs and results (rather than merely process) and evaluates the effectiveness and suitability of controls by contesting the validity of extent processes and procedures, systems and methodologies. A management audit is not designed to merely test and identify conformity and/or non-conformity with existing system requirements, procedures and protocols. The key objectives are to validate the need for existing system requirements, procedures and protocols and, identify key problems areas – or cause and effect patterns. Management audits are generally performed internally – by internal auditors – are essentially systems-based compliance audits.
**Corporate governance audit**

The term corporate governance describes (for our purposes) the processes by which a company is directed, controlled and complies with relevant legislation, extant rules and codes of practice. It is in essence a broad framework of rules and relationships, systems, processes and procedures by which ‘authority is exercised and controlled within a company’, with the generally accepted contemporary principles of corporate governance including:

- the rights of shareholders,
- the interests of other stakeholders,
- the role and responsibilities of the company directors and board members (including nonexecutive directors) and
- company disclosure policies and procedures

A corporate governance audit would include:

- an examination of the general procedures involved in the preparation of company’s financial statements,
- an examination of company internal controls procedures,
- an assessment of the independence of the company external auditors,
- a review of corporate remuneration arrangements for all executive directors, non-executive directors and senior managers,
- an examination of corporate procedures for the nomination of individuals on the board,
- a review of the level of resources made available to directors in perusal of their fiduciary duties and
- an examination of the company procedures for the management of risk

The key objectives of a corporate governance audit are:

- to ensure openness and transparency,
- to promote integrity and honesty and trust and
- to encourage responsibility and accountability, and are generally undertaken by external auditors

**Types of operational audit**

**Risk audit**

A risk audit is an examination of the effectiveness of company processes, procedures and protocols in:

- identifying the nature and contexts of risk (risk identification),
- constructing an effective understanding of its origin and nature (risk assessment),
- developing an appreciation of its implications (risk evaluation) and
- designing effective strategies to manage its consequences (risk management)

Such a risk audit may relate to:
• a category/group/subset of companies possessing common characteristics and/or sharing common attributes,
• a company and/or business type/sub-type within a category/group/subset,
• a cycle of operation within the company and/or business type/sub-type and
• a system within a company’s cycle of operations

A risk audit may, for example, consider:
• the nature of company/cycle/system transactions (for example, the volume of transaction, the value of transaction and the complexity of transactions),
• the adequacy of the company/cycle/system internal controls,
• the nature of the company/cycle/system operating environment,
• the nature of the company/cycle/system regulatory environment and
• the level and adequacy of company/cycles/system resources (including human resources, tangible and non-tangible assets)

Social audit
A social audit is an examination of the extent to which the operations of a company has contributed to social goals of the wider community. Social audits are concerned more with effectiveness rather than efficiency and can be seen as a means of assigning some influence over corporate activities to relevant external stakeholder groups such as employees, consumers and the local community. They provide a framework through which a company can
• identify and qualitatively measure its social performance,
• account for its impact on the community and
• report on that performance to its key stakeholder groups
In a corporate context, social audits remain at a very early stage of development and remain difficult to perform because generally accepted measures of social performance do not exist.

Environmental audit
An environmental audit is an independent assessment of the current status of a company’s compliance with applicable environmental requirements and/or an evaluation of a company’s environmental policies, procedures, practices and controls. In essence, an environmental audit is an examination of a company’s environmental friendliness and concerned primarily with a company’s environmental management systems. Such an audit would review the company’s:
• environmental policies,
• objectives and targets,
• performance procedures and monitoring protocols,
• management review processes

Software Compliance Audit
A software compliance audit involves the identification of software assets, the verification of software assets including licenses and rights of usage and the identification of differences between existing installations and licenses possessed/rights of usage acquired. Such an audit can be a useful means of controlling software installations and lowering the costs of licensing.

**Disaster Recovery and Business Continuity Audit**

Disaster recovery and business continuity refers to company’s ability to recover from a disaster and/or unexpected event and continue operations. An audit of a disaster recovery and business continuity plan would consider, for example,

- how often the disaster recovery plan is updated,
- the appropriateness of hot sites/cold sites,
- the frequency of data and systems backups,
- the location of data and system backups,
- the frequency of disaster recovery procedure tests and drills,
- the composition of the disaster recovery committee and the frequency of systems and documentation updates,
- the availability of hardware and software providers

**Value for money audit**

A value for money audit is an examination of the manner in which assets and resources are allocated and utilised within the business and, as such is concerned primarily with three interconnected and interrelated concepts: economy, efficiency and effectiveness. Although retrospective in nature, the primary objectives of value for money audit are to provide an independent assessment and examination of how economically, efficiently and effectively resources and assets are being utilised and, to offer independent information and advice to companies on how to improve corporate services and competitive performance by adopting value for money policies and procedures. Such a value for money audit may relate to:

- an identifiable cycle of operation within the company and/or business type/sub type (for example, the corporate expenditure cycle) or
- an identifiable system within a company’s cycle of operations (for example, the purchasing system within the corporate expenditure cycle) or
- an identifiable activity within a system (for example, the use of consultants in the purchasing systems within the corporate expenditure cycle)