KASNEB NEW SYLLABUS

GOVERNANCE AND COMPLIANCE AUDIT STUDY TEXT

www.masomomsingi.co.ke

0728 776 317

2021

MASOMO MSINGI PUBLISHERS

PAPER NO. 15

GOVERNANCE AND COMPLIANCE AUDIT

UNIT DESCRIPTION

This paper is intended to equip the candidate with knowledge, skills and attitudes that will enable him/her to effectively plan and conduct a governance and compliance audit.

LEARNING OUTCOMES

A candidate who passes this paper should be able to:

- Identify the objectives and scope of governance and compliance audits
- Design and implement a governance and compliance audit strategy
- Prepare and interpret various governance and compliance audit reports
- Analyse the various checklists/work sheets for governance and compliance audits
- Design self-evaluation tools
- Draft audit report and audit opinion

CONTENT

1. **Basic concepts and elements in auditing**
   - 1.1 Auditing
   - 1.2 Assessment
   - 1.3 Monitoring
   - 1.4 Assurance engagement
   - 1.5 Non-assurance engagement
   - 1.6 Reasonable assurance
   - 1.7 Limited assurance
   - 1.8 Direct reporting engagement
   - 1.9 Attestation engagement
   - 1.10 Compilation engagements
   - 1.11 Assurance reports
   - 1.12 Direct reporting
   - 1.13 Authorities and criteria
   - 1.14 Assertions and audit
   - 1.15 Internal audit
   - 1.16 Statutory audit
   - 1.17 Legal audits

1.18 Governance audit

2. **Governance and compliance risks**

2.1 Identifying, managing and monitoring governance and compliance risks

2.2 Impact of non-compliance: Legal impact, Business impact, Reputational impact

2.3 Role of ethics and compliance officers

2.4 Identify, prioritise, and assign accountability for managing existing or potential threats related to noncompliance or ethical misconduct

2.6 Identifying laws and regulations with which the organisation is required to comply in all jurisdictions where it conducts business, as well as critical organisational policies

3. **Introduction to governance and compliance audit**

3.1 General principles of governance of governance and compliance audit

3.2 The nature and purpose of governance audit

3.3 The nature and purpose of compliance audit

3.4 Types and timing of governance and compliance audits

3.5 Users of governance and compliance audit information and their respective needs

3.6 Qualities of good governance and compliance audit

3.7 The Challenges of governance and compliance Auditing

3.8 Governance and compliance audit in the digital era

4. **Legal, regulatory and professional and ethical considerations**

4.1 Legal requirements on governance and compliance audit for different types of legal entities

4.2 Codes of governance as issued by ICS and different industry regulators

4.3 Regulatory framework of governance and compliance audit industry regulators

4.4 Governance and compliance audit standards by ICS

4.5 Code of ethics for Certified Secretaries

4.6 Auditors' authority, professional liability and legal responsibilities

4.7 Professional objectivity, professional skepticism and professional judgment

4.8 The role of ICS in governance and compliance auditing

4.9 Ethics & integrity as a compliance issue

5. **Engagement and appointment**
   - 5.1 Designing terms of reference
   - 5.2 Designing scope of work and request for proposal
   - 5.3 Tendering and procuring audit services
   - 5.4 Designing proposal
   - 5.5 Qualification requirements
   - 5.6 Negotiating fees amount, structure and timelines
   - 5.7 Acceptance and professional appointments
   - 5.8 Award and execution of contract
   - 5.9 Inception report

6. **Planning for a governance and compliance audit**
   - 6.1 Initial considerations for planning
   - 6.2 Planning process with timelines
   - 6.3 Materiality at planning stage
   - 6.4 Determine audit objective and scope
   - 6.5 Determine the key governance and compliance parameters
   - 6.6 Determining the level of assurance
   - 6.7 Identifying subject matter and criteria
   - 6.8 Understanding the entity and its environment
   - 6.9 Developing audit strategy
   - 6.10 Assessing audit risk, threats and safeguards
   - 6.11 Developing audit plan, programme and procedures
   - 6.12 Preparation of audit working papers
   - 6.13 Developing governance compliance matrix
   - 6.14 Governance and compliance audit checklist
   - 6.15 Quality control
   - 6.16 The audit team

7. **Documentation and Communication**
   - 7.1 Documentation in governance and compliance audit
   - 7.2 Communication between auditor and client organisation

8. **Conduct of governance and compliance audit**
   - 8.1 Inception meeting for clarification and/or understanding of key contact persons, scope, process, timelines, schedule, logistics, operating environment and areas of emphasis

8.2 Reviewing the compliance, governance and internal control systems
8.3 Group governance and compliance audits
8.4 Assessing compliance with the Constitution, applicable laws, rules, regulations, international treaties, international agreements, codes of conduct and internal policies
8.5 Coordination in the conduct of governance and compliance audit
8.6 Role of in-house corporate secretary, internal auditor, external auditor, legal auditor, audit committee, regulatory oversight bodies and other governance assurance functions
8.7 Process of governance and compliance audit
8.8 The governance and compliance audit cycle
8.9 Governance and compliance audit tools
8.10 Use of technology
8.11 Scoring methodology
8.12 Data analysis

9. **Gathering audit evidence**
9.1 Nature and sources of audit evidence
9.2 Types of audit evidence
9.3 Evidence gathering techniques
9.4 Data collection instruments
9.5 Document checklists/list of documents to be provided by client for review by the auditor
9.6 Literature review
9.7 Questionnaire/survey or confidential discussions with select members of the board and senior management using a structured format
9.8 Site visits
9.9 Limitations in gathering audit evidence
9.10 Types of audit tests
9.11 Audit sampling
9.12 Using the work of experts
9.13 Using reports of board evaluation and other internal governance assessments.
9.14 Methods and techniques of auditing high risk areas
9.15 Data analysis
9.16 Evaluating of evidence and forming conclusions

10. **Reporting governance and compliance audit**
    - 10.1 Purpose and users of auditor's report
    - 10.2 Types, contents, elements and structures of auditors' report
    - 10.3 Governance and compliance audit opinion
    - 10.4 Consequences of various audit reports and opinions
    - 10.5 Reporting of suspected unlawful and/or unethical acts
    - 10.6 Conclusions/opinions in governance and compliance audit
    - 10.7 Reports to those charged with governance
    - 10.8 Governance and compliance report on the annual report
    - 10.9 Interim, final and abridged versions of governance and compliance reports
    - 10.11 Submission, presentation and /or filing of audit report
    - 10.12 Closure of the audit assignment
    - 10.13 Audit follow up

11. **Implementing audit recommendations**
    - 11.1 Implementation strategies
    - 11.2 Formulating an action plan and compliance matrix
    - 11.3 Role of the Board in implementing the action plan
    - 11.4 Monitoring, evaluating, tracking progress and embedding recommendations/ decisions arising from the audit.

12. **Post governance and compliance audit**
    - 12.1 Nature and scope of subsequent events
    - 12.2 General guidelines on subsequent events

13. **Peer review mechanism**
    - 13.1 Purpose, scope and types of peer review
    - 13.2 Responsibilities of parties in peer review
    - 13.3 Peer review mechanism stages
    - 13.4 Quality management and assurance measures
    - 13.5 Confidentiality requirements

14. **Governance Awards in practice**
    - 14.1.1 The ICS Governance Awards, other regional governance awards
    - 14.1.2 Parameters evaluated in the governance awards
    - 14.1.3 Award evaluation tool and scoring
    - 14.1.4 Governance Index

CONTENT **PAGE NUMBER**

TOPIC 1

BASIC CONCEPTS AND ELEMENTS IN AUDITING

1.1 Auditing

Auditing typically refers to financial statement audits or an objective examination and evaluation of a company's financial statements – usually performed by an external third party.

Importance of Auditing

Audit is an important term used in accounting that describes the examination and verification of a company's financial records. It is to ensure that financial information is represented fairly and accurately.

Also, audits are performed to ensure that financial statements are prepared in accordance with the relevant accounting standards. The three primary financial statements are:

1. Income statement
2. Balance sheet
3. Cash flow statement

Financial statements are prepared internally by management utilizing relevant accounting standards, such as International Financial Reporting Standards (IFRS) or Generally Accepted Accounting Principles (GAAP). They are developed to provide useful information to the following users:

- Shareholders
- Creditors
- Government entities
- Customers
- Suppliers
- Partners

Financial statements capture the operating, investing, and financing activities of a company through various recorded transactions. Because the financial statements are

developed internally, there is a high risk of fraudulent behavior by the preparers of the statements.

Without proper regulations and standards, preparers can easily misrepresent their financial positioning to make the company appear more profitable or successful than they actually are.

Auditing is crucial to ensure that companies represent their financial positioning fairly and accurately and in accordance with accounting standards.

1.2 Assessment

A compliance assessment is really **a gap assessment**. You are looking to identify gaps between your existing control environment and what is required. It is not a risk assessment, and identified gaps may or may not correlate to risk exposure.

A Compliance Assessment is used to assess and document the current state of compliance oversight, management and related risks in a given compliance area.

The assessment will help identify strengths and opportunities within a specific compliance area's ecosystem, including oversight accountability, regulatory reporting requirements, compliance management, compliance risks, and key compliance gaps, along with laying the groundwork to develop a compliance gap closure plan and escalating compliance concerns as appropriate.

1.3 Monitoring

Monitoring is the regular observation and recording of activities taking place in a project or programme. It is a process of routinely gathering information on all aspects of the project.

To monitor is to check on how project activities are progressing. It is observation; ─ systematic and purposeful observation.

Monitoring also involves giving feedback about the progress of the project to the donors, implementors and beneficiaries of the project.

Reporting enables the gathered information to be used in making decisions for improving project performance.

1.4 Assurance engagement

"Assurance engagement" means an **engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of** the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria.

In some assurance engagements, the evaluation or measurement of the subject matter is performed by the responsible party, and the subject matter information is in the form of an assertion by the responsible party that is made available to the intended users. These engagements are called "assertion-based engagements." In other assurance engagements, the practitioner either directly performs the evaluation or measurement of the subject matter, or obtains a representation from the responsible party that has performed the evaluation or measurement that is not available to the intended users. The subject matter information is provided to the intended users in the assurance report. These engagements are called "direct reporting engagements."

1.5 Non-assurance engagement

Non- assurance engagement is used when **referring to engagements that do not meet the definition** of an assurance engagement. In non-assurance engagement, specific tests to be undertaken the auditor are agreed with the client or user.

Non- assurance engagement is used when **referring to engagements that do not meet the definition** of an assurance engagement. In non-assurance engagement, specific tests to be undertaken the auditor are agreed with the client or user.

1.6 Reasonable assurance

Reasonable assurance is **a high level of assurance regarding material misstatements**, but not an absolute one. Reasonable assurance includes the understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis.

1.7 Limited assurance

Limited assurance means a level of assurance that is less than that provided in an audit. The objective of a limited assurance engagement is a reduction in assurance engagement

risk to a level that is acceptable in the circumstances of the assurance engagement, but where that risk is greater than for a reasonable assurance engagement, as the basis for a negative form of expression of the appointed auditor's conclusion. A limited assurance engagement is commonly referred to as a review.

1.8 Direct reporting engagement

In a direct (direct reporting) engagement, the responsible party does not present the subject matter information in a report in a direct engagement. Instead the practitioner reports directly on the subject matter and provides the intended users with an assurance report containing the subject matter information.

An example of a direct engagement would be a Sarbanes-Oxley engagement to report on the effective control over the financial reporting process.

A direct assurance conclusion would be constructed as: "In our opinion the company maintained, in all material respects, effective internal control over financial reporting as of date/month/year, based on the criteria established in Internal Control – Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)."

1.9 Attestation engagement

In an attestation (also known as assertion-based engagement), the responsible party carries out the measurement or evaluation of the subject matter and reports the information. This subject matter information contains the responsible party's assertion (for example: "The subject matter information is fairly stated as of date/month/year"). The work the practitioner performs is to give an assurance conclusion on this assertion.

1.10 Compilation engagements

A compilation engagement is a type of engagement where a company engages an outside accountant to prepare and present financial statements.

It is not designed to express an opinion or provide assurance regarding the information contained in the financial statement.

The accountant uses financial data provided by the management to compile the required financial statements.

1.11 Assurance reports

An assurance report is the tangible output of an assurance engagement. This report may be for internal use or for external use, but it will always be shared with the person using the information who needs to be confident that it is credible.

Assurance is provided to give its recipients 'piece of mind'. There are different types of assurance reports, they can be for internal and external use, the reports provide confidence to stakeholders in regards to the systems and processes your business has in place. These reports highlight how risks are being managed and steps to take to mitigate them, as well as providing 'good practice' recommendations. The accountants providing you with the report will take different factors into consideration depending on the subject matter and criteria of the report. Assurance reports broadly cover the following:

- The effectiveness of risk management
- Quality of systems and processes in place
- Performance effectiveness of systems and processes
- Specific concerns

1.12 Direct reporting

Direct reports are **employees** who, as the term implies, report directly to someone who is above them in the organizational hierarchy, often a manager, supervisor, or team leader. ... The person in charge of direct reports is responsible for assigning them work and monitoring performance.

1.13 Authorities and criteria

Authority Criteria means such guidelines, criteria and/or application requirements as the Authority may adopt from time to time relating to issuance of revenue bonds for projects such as the Project.

1.14 Assertions and audit

Audit assertions, also known as financial statement assertions or management assertions, serve **as management's claims that the financial statements presented are accurate**.

When performing an audit, it is the auditor's job to obtain the necessary evidence to verify the assertions made in the financial statements.

Assertions are claims that establish whether or not financial statements are true and fairly represented in the process of auditing.

Assertions are an important aspect of auditing. Since financial statements cannot be held to a lie detector test to determine whether they are factual or not, other methods must be used to establish the truth of the financial statements.

Assertions are defined as "a statement that is believed to be true by the speaker. "An assertion can be anything, e.g., "I assert that fundamental value investing is the best investing philosophy."

However, it is difficult to measure whether the statement is indeed true. Similarly, with financial statements, it is difficult to determine what financial information is free from material misstatement.

There are two aspects to material misstatement. Clearly, materiality plays a large role; however, how to measure what information is true and fair or misstated is crucially important.

Assertions play a key role in determining what is true and fair when auditing financial records.

1.15 Internal audit

Internal audits evaluate a company's internal controls, including its corporate governance and accounting processes. These audits ensure compliance with laws and regulations and help to maintain accurate and timely financial reporting and data collection. Internal audits also provide management with the tools necessary to attain operational efficiency by identifying problems and correcting lapses before they are discovered in an external audit.

The role of internal audit is to provide independent assurance that an organisation's risk management, governance and internal control processes are operating effectively.

1.16 Statutory audit

A statutory audit is **an independent process of determining whether an organisation's financial statements give a true and fair view of its financial performance and financial position**. A statutory audit is not, as some would assume, a search for the proverbial needle in a haystack.

1.17 Legal audits

Legal auditing is a litigation management practice and risk management tool, used by insurance and other consumers of legal services, to determine if hourly billing errors, abuses, and inefficiencies exist by carefully examining and identifying unreasonable attorney fees and expenses.

1.18 Governance audit

Governance Audit: **an objective review of how an organization is governed**. This review looks at how the governance structure is designed, but also how it is actually operating. It assesses whether there adequate checks and balances in place for effective governance.

TOPIC 2

GOVERNANCE AND COMPLIANCE RISKS

2.1 Identifying, managing and monitoring governance and compliance risks

Compliance risk is an organization's potential exposure to legal penalties, financial forfeiture and material loss, resulting from its failure to act in accordance with industry laws and regulations, internal policies or prescribed best practices. Compliance risk is also known as *integrity risk*.

Organizations of all types and sizes are exposed to compliance risk, whether they are public or private entities, for-profit or nonprofit, state or federal. An organization's failure to comply with applicable laws and regulations can affect its revenue, which can lead to loss of reputation, business opportunities and valuation.

Types of compliance risk

An organization may be implicated in the following types of compliance risks:

- **Corrupt and illegal practices.** Legal compliance ensures that the organization, its agents and employees are abiding by the laws and regulations of the industry. Common compliance risks involve illegal practices and include fraud, theft, bribery, money laundering and embezzlement.
- **Privacy breaches.** A common compliance risk is the violation of privacy laws. Hacking, viruses and malware are some of the cyber risks that affect organizations. Additionally, if a company handles sensitive information, it is required to take the appropriate measures to protect that data and prevent privacy breaches.
- **Environmental concerns.** These compliance risks deal with pollution and environmental damage an organization's operations can cause. Examples include the destruction of natural habitats, use of harmful chemicals, hazardous waste disposal and pollution of groundwater. Many companies are integrating sustainability into their business strategies and are providing their employees with training and resources to help them achieve environmental compliance.