June 2011

Compliance Guidance

Principle 6.1
The board should ensure that the company complies with applicable laws and considers adherence to non-binding rules, codes and standards.

Each organisation should establish and maintain a compliance framework and process that is appropriate taking into account the laws, rules, codes and standards that are applicable in the light of compliance risk profile of the particular organisation. Consideration should be given to the approach that is adopted in addressing compliance in relation to an organisation's ethics and risk management framework.

Target audience

This practice note is intended to provide guidance to the board and management in discharging their responsibilities relating to compliance with applicable laws, rules, codes and standards. It describes practical considerations that should be taken into account in the governance of compliance and is aligned with South African Generally Accepted Compliance Practice[1].

Introduction

All organisations must comply with applicable laws, rules, codes and standards. In order to achieve this objective, it is necessary to establish a compliance framework and process that is appropriate for the organisation. Ultimate responsibility for understanding and overseeing the management of compliance with applicable laws, rules, codes and standards resides with the board. Of necessity, responsibility is delegated to management to undertake business activities in compliance with laws, rules, codes and standards.

Responsibility for assisting management/the board in terms of the aforementioned should be specifically assigned.

In some industries/organisations this is particularly well developed and is typically called the compliance function.

It is recognised that organisations may not have formally established a compliance function or appointed a compliance officer and that certain aspects of the compliance process may be undertaken by various role players e.g. legal, company secretary, risk, internal audit.

Notwithstanding the matters discussed above, organisations should have an effective compliance framework and process that has the capacity and resources to assist management/the board to achieve compliance objectives.

The development of a fully effective compliance function, however structured, can take some time before the value thereof is realised. This

[1] Compliance Institute of South Africa, 2007

may take up to 5 years, particularly, from an organisational development and compliance culture perspective.

A compliance function requires the appropriate status and independence.

Compliance officers are faced with the challenge of balancing the role of assisting management/the board with their assurance role in terms of which feedback is provided to various stakeholders relating to the level of compliance.

It is recognised that the development and maintenance of a compliance culture is essential. This can be described as a pervasive belief by organisational stakeholders that business activities must be conducted in compliance with all laws, rules, codes and standards. This will require appropriate support from management/the board within an organisational structure that promotes compliance underpinned by an effective compliance process.

The organisation's control framework/procedures should have the necessary compliance requirements embedded therein.

1. Governance

Ultimate responsibility for understanding and overseeing the management of compliance with applicable laws, rules, codes and standards resides with the board and this should be recognised in the organisation's governance structures.[2]

The organisation's governance structures should be designed in such a way as to enable the board to:

- Be aware of the laws, rules, codes and standards applicable to the organisation, as well as their impact on the organisation and who the relevant supervisors/regulators are;
- Understand the organisation's compliance framework and its role and accountability relating thereto;
- Approve and regularly review the compliance policy;
- Keep up to date with changes in the regulatory environment;
- Assess and understand the organisation's compliance with laws, rules, codes and standards;
- Recognise the compliance function as part of the overall risk management framework;
- Ensure that management effectively and appropriately reports the results of compliance monitoring throughout the organisation;
- Confirm that the compliance framework is regularly reviewed and aligned with the organisation's strategic goals;
- Ascertain that material compliance issues are afforded the necessary focus;
- Ensure that management resolves compliance issues effectively and timeously;
- Enable the compliance function to be sufficiently independent of management and other functions, e.g. internal audit;
- Provide adequate support for the compliance function, i.e. financial and other;
- Monitor that the organisation's remuneration and reward system takes cognisance of and supports a compliance culture;
- Monitor that the desired compliance culture is established;
- Take cognisance of and adhere to any relevant laws relating to the implementation, management and oversight of the compliance function;

It is advisable to make use of a phased approach in the implementation of a compliance framework and process. This should be underpinned by the development, approval and implementation of a compliance policy, charter and manual, which will serve as a platform to institutionalise a compliance process. The identification and assessment of compliance risks can take some time to complete and should be undertaken with a view to enabling the organisation to manage its business in compliance with applicable laws, rules, codes and standards.

The organisation's responses to the aforementioned should be appropriate to its particular circumstances. This should be aimed at providing reasonable

[2] Generally Accepted Compliance Practice framework Principle and Standard 1

assurance that business will be conducted in compliance with applicable laws, rules, codes and standards.

Once the organisation's risk responses have been appropriately addressed in respect of the assessed regulatory universe, it will then be in a position to conduct a review of its business activities to assist management and the board to determine whether the applicable requirements have been adhered to.

Compliance reporting is an important element of all the aforementioned phases of the compliance process. This may take some time to be fully developed.

2. Framework

Each organisation should design, develop, implement and maintain a compliance framework which will be appropriate for its circumstances. This will include a compliance policy, charter, manual and organisational structure that supports a compliance culture.

In summary, the compliance policy addresses strategic compliance matters and the organisation's commitment to compliance, while the compliance charter will serve as a terms of reference for the compliance function. A compliance manual will typically describe the organisation's compliance framework and process and provide a description of how compliance is undertaken within the organisation, as well as specifications relating to roles and responsibilities of stakeholders.

2.1 Compliance policy

The board should ensure that there is a written compliance policy that describes the organisation's commitment and approach to compliance and that it is implemented, supported and adhered to.

The compliance policy is typically drafted by a compliance officer with input from compliance stakeholders for submission to the board for approval. Such approval will give it the status required for effective implementation. This policy will formally communicate the organisation's philosophy and approach to the management of compliance risk and to formalise the establishment of a compliance framework and process.

The Compliance Policy is an important source of information regarding compliance and should be widely distributed throughout the company. Care should also be taken to make this a user friendly and accessible document.

Organisations should develop policies using their particular policy format, but should include the following:

- **Compliance policy statement**
  A statement that clearly specifies the organisation's commitment to compliance and the strategic positioning thereof. Refer to Appendix A for a suggested compliance policy statement.

- **Rationale for compliance**
  An explanation of why compliance with laws, rules, codes and standards is needed.
- **Establishment of a compliance function**
  A high level description of the compliance function and the framework and process adopted.
- **Roles and responsibilities of key role players**
  A high level description of the roles and responsibilities of key role players. Including the board, board committees, management, compliance function and staff.
- **Compliance approach**
  An indication of how the organisation complies with both the spirit and the letter of applicable laws, rules, codes and standards.

2.2 Compliance Charter

The compliance terms of reference, compliance principles and roles and responsibilities of the compliance function and other compliance stakeholders may be set out in a Compliance Charter. This is a document that supports the organisation's compliance philosophy, which is endorsed by management and which confirms the authority of the compliance function, as well as management's support thereof.

Where a separate compliance charter[3] is developed, refer to Appendix B for the typical content thereof.

The compliance policy and charter should specifically address the independence of the compliance function.

2.3 Compliance Manual

Organisations should develop a compliance manual that describes the compliance framework and process, as well as key matters relating to the implementation thereof.

The compliance function is normally responsible for drafting and maintaining a compliance manual with input from key stakeholders and support from management. This will serve as a method of work for the compliance function and the respective compliance role players. Compliance manuals may also include the compliance management plans that are developed in respect of the applicable regulatory requirements. These are, in essence, an identification, analysis and assessment of regulatory requirements together with the identification controls that are required to ensure compliance.

A compliance manual should:

- Contain a description of the compliance framework and process;

[3] A separate compliance charter may not be required where the compliance policy and/or manual provides adequate specification of the compliance function terms of reference and the roles and responsibilities of compliance stakeholders.

- Refer to material laws, rules, codes and standards that are applicable;
- Address all material regulatory risks that the organisation faces;
- Address procedures and controls relating to laws, rules, codes and standards;
- Be readily available;
- Be reviewed and updated routinely (at least annually).

Refer to Appendix C for the suggested contents of a compliance manual.

Applicable laws, rules, codes and standards should be addressed at an operational/procedural level within the compliance framework. This may be incorporated as part of the compliance manual and within the organisation's compliance risk management plans.

3. Structure

Principle 6.4
The board should delegate to management the implementation of an effective compliance framework and processes.

As previously stated, the board is ultimately responsible for compliance.

Of necessity, responsibility is delegated to management to undertake business activities in compliance with laws, rules, codes and standards. A permanent and effective compliance function should be established. The structure thereof should be appropriate to the size of the organisation.

The compliance function should be established and maintained in a way that ensures it is able to discharge its responsibilities effectively. This is dependent on the status and standing of the function which will require adequate resources, supported by a framework and process that is embedded in the day to day activities of the organisation.

In order to provide the board with reasonable assurance that the organisation complies with laws, rules, codes and standards, there should be an effective compliance reporting process which addresses all significant risks, exposures and matters that require management attention. A number of different stakeholders may be involved in the aforementioned. However, the compliance function should co-ordinate such reporting.

Organisations may structure there compliance function according to a centralised or decentralised model. The approach that is adopted should provide the compliance function with a sound platform to achieve its objectives.

In a centralised compliance function the compliance resources would be concentrated in a central (group) compliance office with responsibility for the management of compliance risk throughout the organisation.

In decentralised compliance functions, there is usually a relatively small central (group) compliance function whose main role may be the setting of

group policies and consolidation of business unit compliance reports into a group report. Each business unit would typically establish their own compliance function which has a dotted line reporting responsibility to the central (group) compliance function.

It is noted that in some organisations the compliance framework may have elements of both centralised and decentralised compliance functions.

A person should be appointed with responsibility for managing the compliance function. This person should have the appropriate seniority, knowledge, skills and experience to assist management/the board to discharge their responsibilities relating to compliance.

Importantly, compliance officers should be adequately independent to discharge their responsibilities objectively as an internal assurance provider in conjunction with internal audit and other role players, i.e. relating to compliance with laws, rules, codes and standards.

The compliance function head would typically report to a committee that is independent of executive management and have direct access to the chief executive of the organisation. Importantly, the compliance function may report to management, but would need to be adequately independent and be seen to be adequately independent.

4. Process

Key aspects of the compliance process are set out under appropriate headings in this section. In terms of Generally Accepted Compliance practice, this is structured in four phases:

- Compliance risk identification;
- Compliance risk assessment;
- Compliance risk management;
- Compliance monitoring.

The aforementioned are explained hereunder together with commentary covering compliance reporting and the management of the relationship with supervisors/regulators.

Compliance management responsibilities should be addressed in terms of a compliance programme. The compliance programme should incorporate planned compliance activities, including implementation and review of specific policies and procedures, compliance risk identification and assessment, compliance monitoring, reporting, management of the relationship with regulators, and training. The programme should be risk-based and subject to appropriate review and approval. The compliance programme should be co-ordinated with the plans developed by the organisation's internal and external assurance providers.

The role played by the compliance function should be focused on pro-active assistance to management through the provision of compliance products and services.

Compliance Risk Identification and Assessment

Risk identification involves the establishment of an organisation's regulatory universe, which includes the identification of all laws, rules, codes and standards that are applicable. This should be assessed using an appropriate risk rating methodology with a view to prioritising management's attention thereto.

The compliance universe is an effective tool which can be used to formally present an organisation's compliance management priorities to the board and management.

Compliance Risk Management

An organisation's control framework will, inter alia, be designed to provide reasonable assurance that its business activities will be conducted in compliance with laws, rules, codes and standards. The importance of addressing the aforementioned at an operational level cannot be overstated. The adequacy and effectiveness of compliance related controls should be a specific management focus.

Compliance risk management plans are a valuable tool in indentifying specific sections of laws, rules, codes and standards that are applicable to

the organisation and for analysing the aforementioned in plain language, assessing the risk thereof, identifying controls that will provide reasonable assurance of compliance therewith and for establishing management priorities or actions required.

Risk management plans may also be used to establish monitoring priorities and to track management initiatives relating to laws, rules, codes and standards.

Management is responsible for compliance. The compliance function assists management to discharge their responsibilities and compliance risk management plans play a central role in this regard.

Compliance Monitoring

Compliance monitoring is an essential part of the compliance process. It is undertaken by various stakeholders including management, compliance, internal audit, other internal assurance providers, as well as external assurance providers. It may be formal or informal in nature.

As recognised in Chapter 4 (The Governance of Risk) of King III, the audit committee should ensure a combined assurance model is applied. This is certainly applicable in respect of compliance assurance where the management, internal and external assurance providers should work in unison.

Both routine and independent compliance monitoring should be undertaken in the achievement of monitoring objectives as part of a co-ordinated monitoring programme. Importantly, routine compliance monitoring that is undertaken by management as part of the ongoing business activities of an organisation plays a valuable role in first line of defence assurance.

The compliance function should facilitate and/or develop a monitoring programme which addresses monitoring plans in the short and longer terms. It should be risk based with high risk areas subject to more intensive monitoring than low risks areas. This programme should be formally approved in advance of its implementation.

The compliance function should be subject to regular independent review.

Compliance Reporting

The contribution of both formal and informal compliance reporting should be recognised within the compliance framework of an organisation. This will involve various compliance role players, such as the board, board sub-committees, management, internal audit, the legal function, risk stakeholders and should be tailored to meet the needs of the organisation.

Compliance reporting should be adequate to provide management and the board with information that will provide the support necessary to discharge their respective responsibilities.

Compliance reporting should be undertaken in a manner that is appropriate for each organisation's circumstances. Management should undertake routine compliance monitoring as part of their ongoing management responsibilities. This should identify compliance risk, exposures and breaches which should be appropriately reported within the organisation's governance structures. Responsibilities relating to the aforementioned should be identified and corrective action addressed as appropriate in compliance reports.

The compliance function plays a central role in co-ordinating the compliance reporting within the organisation, including receiving reports from management relating to compliance, collation and summary thereof for reporting to executive and board committees.

The compliance function may also prepare reports relating to monitoring that is undertaken by the compliance function and other stakeholders.

Further, reporting relating to new and existing laws, rules, codes and standards should be prepared in order to provide management/the board and staff members with appropriate support relating thereto.

In view of the increasing volume and complexity of the universe of regulatory requirements, a risk based approach to compliance management should be adopted. While all applicable laws, rules, codes and standards must be complied with, management attention should be focussed on the higher risk requirements and the aforementioned compliance reporting should address all significant compliance risks, exposures and breaches.

Management action required relating to the above should be suitably addressed and the board should be provided with adequate information that will facilitate appropriate evaluation of the compliance risk profile of the organisation.

Management of the relationship with supervisors/regulators

The management of the relationship with supervisors/regulators should be subject to appropriate oversight and control by the board.

Where statutorily required, the organisation will routinely report the status of the organisation's compliance to the relevant supervisors/regulators in the prescribed format. Management responsibilities relating to such reporting and other aspects of the relationship with supervisors/regulators should be clearly defined.

5. **Culture**

Compliance culture is defined as the culture of shared values, beliefs, assumptions and behaviours that all business should be conducted in compliance with laws, rules, codes and standards.

As stated in King III (Chapter 6), a compliance culture should be encouraged through leadership, establishing the appropriate structures, education and training, communication and measurement of key performance indicators relevant to compliance. Compliance is most effective in a corporate culture that emphasises honesty and integrity and in which the board consistently leads by example.

The compliance function assists with the fostering of a compliance culture that engenders an awareness and recognition of the value of compliance risk identification, assessment, management, monitoring and reporting as part of ongoing activities.

The board is responsible for the development and maintenance of a compliance culture which will depend on the recognition of the need for compliance in an organisation's strategy, supported by appropriate organisational structures and, importantly, adequate focus thereon in the control framework.

The compliance policy, which is approved by the board and endorsed by top management, should indicate the organisation's expectations of all staff regarding their obligations relating to compliance with laws, rules, codes and standards, including the desired standard of conduct and the desired culture of the organisation. Management should be seen to be actively implementing and adhering to the desired standards of conduct and values.

Induction training should include the responsibility of all staff to comply with laws, rules, codes and standards. Importantly, compliance training programmes should not only be aimed at making employees aware of their obligations in respect of specific laws, rules, codes and standards, but should also seek to promote the desired culture and create an awareness of the overall compliance framework in the organisation.

Behaviour that supports compliance with regulatory requirements should be encouraged and behaviour that compromises this should not be tolerated. There should be consistency in the approach to reward systems and disciplinary action for compliance/non-compliance at all levels in the organisation. An organisation's disciplinary policies and procedures should specifically address non-compliance with laws, rules, codes and standards.

An appropriate compliance culture will reduce compliance risks. It is anticipated that regulators will consider the culture of organisations when assessing their regulatory risks.

Note:

The compliance function should not be regarded as a "policeman" or internal auditor divorced from the organisation, but rather the function to assist management and the board to comply with laws, rules, codes and standards.

Appendix A

Suggested Compliance Policy Statement[4]

[Insert name of organisation] recognises its accountability to all its stakeholders under the legal and regulatory requirements applicable to its business and is committed to high standards of integrity and fair dealing in the conduct of its business. We are committed to complying with both the spirit and the letter of applicable requirements and to always act with due skill, care and diligence. The Board/Partners/Trustees/Members of [insert name of organisation] are ultimately accountable to its stakeholders for overseeing compliance requirements.

The responsibility to facilitate compliance throughout [insert name of organisation] has been delegated to the appointed Compliance Officer [insert compliance officers name] [Where an independent compliance practice has been appointed the Compliance Officer, the title and name of the internal manager who has compliance responsibility should be inserted] who supervises the Compliance Function. The Compliance Function identifies, assesses, advises on, monitors and reports on the regulatory Compliance Risk of [insert name of organisation]. The management of Compliance Risk forms part of the overall risk management framework of [insert name of organisation].

The Compliance Officer is responsible for the effective implementation of the Compliance Policy.

However, it must be emphasised that the primary responsibility for complying with any regulatory requirement lies with all members of staff conducting the particular transaction or activity to which regulation applies. All relevant staff must therefore be conversant with appropriate legislation and subordinate regulations, conditions and rules promulgated by regulators as well as with the compliance manual and/or technical guidance notes applicable to their specific area of responsibility. Members of staff are expected to comply both with the letter and with the spirit of these requirements.

Compliance risks are the loss of reputation, fines, civil claims, and/or loss of authorisation by the regulators, which would jeopardise the business of [Insert name of organisation]. If the key legislation governing our business is breached, the organisation could be fined severely and the Compliance Officer could be imprisoned. Damage to the organisation's reputation could result in an exodus of clients. Compliance risks are serious and need to be controlled by all individuals in the organisation.

The Compliance Charter sets out our approach to managing our compliance risks. Further guidance and procedures can be found in the compliance manual.

4 A standard compliance policy cannot be used by all organisations owing to differences in philosophy, approach and mission.

Any breach of this Compliance Policy is considered serious and remedial action will result in disciplinary action that could ultimately lead to dismissal of the offender.

Reporting Lines

The Compliance Officer on behalf of the Compliance Function reports to the Chief Executive Officer [or insert other appropriate function]. In addition, the Compliance Officer reports to [the risk committee/audit committee or another relevant assurance committee]. More detail regarding the compliance reporting lines within the organisation are set out in the Compliance Charter (See Compliance Structures and Responsibilities in Compliance Charter Guideline).

Appendix B

Suggested contents of a compliance charter

1. **Compliance Function**

1. Compliance Risk
Explain compliance risk, the consequences of non-compliance and the organisation's approach to managing these risks.
2. Compliance Philosophy
Provide details of the organisation's perspective on compliance, including core values such as integrity, fair dealing, accountability, transparency as well as the organisation's compliance risk tolerance.
3. Independence
Explain that the compliance function is independent of business activities and needs to function adequately, independently and objectively in order to achieve its objectives.
4. Management Support
Affirm that the compliance function will have access to and demonstrable support from management/Board. Detailed reporting lines should also be included.
5. Authority
Detail the rights and powers of the compliance function:
- Access to:
    - all functions;
    - records and personnel;
    - all relevant committees;
    - agenda and minutes of executive, management and board meetings;
    - reports and correspondence with regulators;
    - external and internal audit reports;
    - any report from any person on a compliance matter.
- Assistance that can be expected from staff when undertaking monitoring reviews;
- To direct and require staff to apply the compliance policy and standards.

6. Remedial Action
Explain that all staff are required to comply with both the letter and the spirit of the law and that failure to do so will result in disciplinary procedures.

2. **Compliance Structure**

Detail the format of the compliance structure and the principles thereof that will enable the compliance function to:
1. *Provide management/the board with regular information regarding the level of compliance;*
2. *Have adequate resources;*
3. *Function adequately, independently and objectively;*
4. *Ensure no conflicts of interest exist with other assurance functions;*

5. *Report issues of non-compliance in a timely manner;*
6. *Have direct access to the CEO;*
7. *Liaise directly with the regulators with regard to reporting required.*

3. **Compliance Responsibilities**

1. Introduction
   Provide details of parties responsible for compliance and the core responsibilities of the compliance function.
2. Board of Directors and Executive Management
   Communicate the responsibilities of management, board, CEO, etc and the authority delegated to the compliance function.
3. Compliance Function and Compliance Officers
   Confirm the roles and responsibilities of the compliance function with regard to:
   - setting policies;
   - providing advice;
   - designing and implementing the compliance risk management framework;
   - identifying the regulatory universe;
   - compiling a compliance manual;
   - establishing and maintaining a compliance culture;
   - monitoring;
   - reporting to management/board.

4. **Letter of Endorsement from the CEO**

This should be a letter from the CEO detailing the organisation's commitment to compliance, compliance philosophy, risk tolerance and management/board support for the compliance function.

Appendix C

Suggested contents for a Compliance Manual

Introduction and Background Information

- the reasons for establishing an independent compliance function;
- what compliance is;
- what the compliance function is;
- management's commitment to fostering a culture of compliance with relevant regulatory requirements;
- a summary of the compliance charter and compliance policy regarding management's commitment, definitions, policies, objectives and standards;
- relevance and roles of relevant supervisory bodies.

Management/Board Resolution

This section should demonstrate that management/board understand their responsibilities regarding regulatory requirements and that they have taken the necessary actions to ensure they meet their obligations. Much of this should be extracted from the Compliance Charter and Compliance Policy.

In this regard, the following should be included:

- management/board endorsement of the Compliance Policy;
- commitment to complying with Regulatory Requirements and internal policies;
- process for dealing with instances of non-compliance.

Management/board resolutions provide the Head of Compliance with the authority to implement the necessary compliance programme and facilitate corrective measures. They also illustrate commitment to effective compliance systems throughout the organisation from management/board down.

Compliance Function

This section should contain the following:

- roles and responsibilities of all staff who are involved in the compliance process;
- structural arrangements for the compliance function, including reporting lines, access to information, whistle-blowing and escalation procedures
- process to evaluate compliance, or details of the compliance programme.

Statutory, Regulatory and Supervisory Requirements

This section focuses on operational procedures. It should focus on the operational procedures around the regulatory requirements that fall within the scope of the compliance function. It can be extracted from the compliance risk Management Plans and should include:

- A summary of the requirement, its impact on the business and the potential results of non-compliance. This should not be seen as a replacement for the regulatory requirements, but rather the organisation's summary of them;
- A description of internal procedures designed to ensure compliance with the requirement;
- A description of the monitoring and review procedures to evaluate the organisation's compliance with the requirement.

Reference Points

This section should provide users of the compliance manual with access to the regulatory requirements contained in the manual, access to the appropriate compliance officer in the organisation, escalation procedures and whistle-blowing procedures.

The compliance manual should cover all matters relating to compliance for the organisation. It should be simple, but not simplified or simplistic, in order to ensure its implementation. Furthermore, it should be easily accessible to all.

In order to encourage its implementation, there should be training of all relevant staff regarding its contents and its application.

Resources

This practice note was drafted in conjunction with the Compliance Institute of South Africa.