SECTION 2

1. INTRODUCTION

1.1 Background to compliance in South Africa

1989   South African Futures Exchange Rules - requires member firms to have appoint a registered compliance officer. The compliance officer was responsible for ensuring that the member firm complied with the SAFEX rules.

1994   King I — highlights the importance of governance and compliance

1995   Johannesburg Stock Exchange Rules - requires member firms to employ the services of a registered compliance officer. The main responsibility of the compliance officer, at this time, was to ensure the member firm complied with the JSE rules.

1999   Strate Rules — requires the appointment of a registered compliance officer.

2000   South African Reserve Bank, Banking Supervision introduces Regulation 47 to the Banks Act. This regulation required all South African banks and foreign banks with South African branches to establish a compliance function. It details the roles and responsibilities of this function, but leaves ultimate responsibility for compliance in the hands of management.

2002   King II — again highlights the importance of governance and compliance.

2004   Financial Advisory and Intermediary Services Act — requires all licensed Financial Service Providers to appoint an approved compliance officer. The compliance officer can either be an employee or an outsourced compliance practitioner.
1.2 Benefits

The establishment of an independent Compliance Function holds, *inter alia*, the following benefits for the entity:

(a) Lower impact of reputational risk due to, *inter alia*, a specific focus on:
- maintaining the highest personal standards of integrity at all levels;
- the importance of true and fair dealing with all clients;
- the provision of qualitative and competent services;
- putting the entity's interests above those of individual employees.

(b) Lower impact of regulatory risk due to a continuous focus and/or awareness on compliance to all applicable laws, regulations and supervisory requirements.

1.3 Conclusion

The implementation of an independent compliance function is a requirement of new legislation and is in line with international developments. This will definitely have a positive effect on the impact of compliance risk on an organisation.
1.4 The need for compliance

The reasons for establishing an independent compliance function include the following:

(a) To comply with relevant legislation
Regulation 47 of the Banks Act No 94 of 1990 and the Financial Advisory and Intermediary Services Act No 37 of 2002 (FAIS) stipulate that an independent compliance function must be established in banking and financial services organisations respectively.

(b) To provide for a formal and structured monitoring of compliance
A compliance manual provides for a specific compliance monitoring process that should not only be formal, but also structured and therefore more visible to all the relevant stakeholders.

(c) To facilitate the establishment and enhancement of a compliance culture
A compliance culture can only be established effectively if staff members perceive compliance as being more than just manuals and checklists. Staff members must realise that an effective compliance system depends on a continuous awareness of compliance issues, which should be one of the Compliance Function's main responsibilities.

(d) To co-ordinate all the relevant compliance functions within the Group
The establishment of a central and independent Compliance Function at Group level should enhance effective co-ordination of compliance strategies throughout the business.

(e) To give specific focus to compliance risk within a broader risk management framework
The Compliance Function is ideally positioned to deal with compliance risk as part of operational risk that should fall within the scope of the bigger risk management strategies.

(f) To be in line with international developments/trends
Compliance Functions have been established at most of South Africa's international competitors and/or trading partners. Local business must follow suite if they intend to retain, or improve, their international competitive edge.

(g) Benefits
The establishment of an independent Compliance Function provides, inter alia, the following benefits:

(i) Lower impact of reputational risk due to a specific focus on: - Maintaining the highest personal standards of integrity at all levels; - The importance of honest and fair dealing with all clients; - The provision of qualitative and competent services; - Putting the business interests above those of individual employees.

(ii) Lower impact of regulatory risk due to a continuous focus and/or awareness on compliance to all applicable regulatory requirements.

(h) Conclusion
The implementation of an independent compliance function is a requirement of new legislation and is in line with international developments. This will definitely have a positive effect on the impact of compliance risk on the business.
1.5 Why comply

(a) Introduction
Broadly speaking, there are two reasons why a business should comply with regulatory requirements.
Firstly, because it is the law, and secondly, because it makes good business sense!
(b) It is the law
Business does not, from a legal standpoint, have any choice as to whether they should or should not comply with the regulatory requirements - they are obliged to comply. Failure to comply is likely to result in appropriate sanctions being imposed.
(c) Good Business Practice
Compliance with regulatory requirements makes good business sense. In the final analysis, there is a direct link between client satisfaction and confidence and the businesses that observe the applicable regulatory requirements. These two aspects will be considered:

(i) Client satisfaction
The Financial Advisory and Intermediary Services Act (FATS), which regulates the giving of advice and the rendering of financial services, prescribes, inter alia, that:
- The business must conduct a needs analysis to determine what the clients financial needs are; and
- Certain information must be disclosed to the client regarding the financial products that are being offered to the client, the supplier of the financial services and the financial services provider itself.

The above requirements represent good business practice. Client satisfaction is likely to be higher in instances where a needs analysis has been conducted, where documents have been completed in full and the appropriate products have been satisfactorily explained to the client. Further, satisfied clients make referrals that will lead to improved business opportunities.

(ii) Client confidence
Business is required to comply with minimum capital adequacy and liquidity requirements. Knowing that a business complies with these minimum requirements provides the client with confidence that the business they are dealing with is financially sound. There have been a number of high profile business failures in recent years, notably:
- Enron
- WorldCom
- Allied Irish Bank
- Barings Bank
- BCCI
- Beige
- LeisureNet
- Saambou Bank
2. IDENTIFICATION OF KEY ROLE-PLAYERS

Before addressing the regulatory environment in the broader context, it is useful to identify the key compliance role-players.

2.1 Role Players

Although ultimate accountability for compliance with the legal and regulatory requirements rests with the Board of Directors, compliance is a multidisciplinary process in which, at a bare minimum, the following role-players should be involved:

Board of Directors;
Audit Committee;
Chief Executive Officer/Executive Management Committee;
Line Management and/or Boards for Divisions and Subsidiaries;
Internal Audit function
Compliance Function;
External Audit function;
All employees; and
Regulators.

General guidelines for the roles and responsibilities of each of these role-players, with specific reference to compliance, are briefly described in the following sections.

(a) Board of Directors

The Board is appointed by and accountable to its shareholders to lead, control and monitor the business of the Group and to provide effective corporate governance, with the specific responsibility to oversee compliance with, regulatory requirements.

(b) Audit Committee

A special sub-committee of the Board is established to oversee compliance matters. This Committee is a very important part of the whole compliance system and monitors compliance at the highest level.

(c) Executive Management Committee

The Executive Management Committee (EXCO) is appointed by the Board to manage the business within an acceptable risk profile and to achieve sustainable profits. Its specific responsibility regarding compliance must be to ensure that risk processes, with regard to regulatory requirements, are implemented.

(d) Line Management and/or Boards for Divisions and Subsidiaries

Line Management and/or Boards for Divisions and Subsidiaries accept responsibility for the risks undertaken in their divisions and/or subsidiaries within the confines of the overall risk control framework of the business. Their specific responsibility regarding compliance includes the implementation of compliance procedures to ensure adherence to relevant regulatory requirements.

(e) Internal Audit Function

Although there is common ground between the Compliance and Internal Audit Functions, the focus of the respective functions is different. The role of Internal Audit in this regard, is to review the existence and adequacy of management control systems to ensure proper compliance with laid down policies, plans, procedures and regulatory requirements. As a result of the work of Internal Audit, the Compliance Function can, in certain instances, rely on work carried out by Internal Audit instead of carrying out compliance reviews on their own. On the other hand, Internal Audit can consult with the Compliance Function in identifying high-risk areas in the planning of audits.
An additional check would be for the Internal Audit Manager, as part of their normal audit responsibility, to review certain aspects of the work carried out by the Compliance Officer. Due to the overlap between the Audit and Compliance Functions, a sound and an interactive relationship between the two must be maintained.

(f) Compliance Function

The Compliance Function is an independent function, which is associated with all aspects of compliance, including the monitoring of the compliance risk processes. It is imperative that the Compliance Officer has the necessary rights and powers to fulfil this role impartially and effectively.

Further responsibilities of the Compliance Officer can be divided into the following main areas:

(i) **Standard setting**
   Set standards for achieving compliance with the relevant regulations; ensure that these standards and other compliance principles are effectively communicated; secure the commitment of Executive Management for the application of these standards and finally ensure consistency of approach and practice.

(ii) **Providing advice**
   Provide a central point of reference and expertise in compliance-related matters and, in particular, advise on the policy and strategic decisions that might have compliance implications. An example of this would be to provide an independent view in the formulation or amendment of the policy regarding the managing of conflict of interest.

(iii) **Monitoring**
   The implementation of the entire compliance process and the subsequent monitoring of the level of compliance within the business is the responsibility of this Function — refer to Section 13 for a more detailed description of this process.

(iv) **Maintaining external relations**
   The Compliance Officer must strengthen the working relationship with the Regulators appropriately by:
   - Being the senior point of contact with the Regulators;
   - Collating, co-ordinating and representing the business's views on sector and industry-wide matters by direct representation to the Regulators; and;
   - Liaise with relevant internal, as well as external stakeholders.

(v) **Resolving issues of non-compliance**
   The Compliance Officer is not only responsible for the reporting of issues of non-compliance through to the monitoring process (refer Section 13), but is also required to resolve issues of non-compliance efficiently and effectively. Depending on the seriousness and impact of the specific non-compliance, this could involve facilitating the process of ensuring the necessary and the responsible line manager implements appropriate corrective measures.

(vi) **Training**
   The Compliance Officer is also, as part of the responsibility to enhance a compliance culture, responsible for promoting an effective compliance system through appropriate training interventions and awareness campaigns. These interventions will vary from brief discussions to more detailed and comprehensive programmes with the intention to keep
employees informed and abreast with developments in the compliance field.

(vii) **Assisting with ad hoc investigations**
Given the strategic position of the Compliance Officer and their specific field of expertise, they may be requested to become involved in multi-disciplinary projects e.g. assisting in due diligence reviews and/or strategic planning sessions.

(g) **External Audit Function**
The External Auditors are required to review the risk processes as part of their statutory audit duties imposed on them by the Companies Act, Banks Act and any other applicable legislation.

(h) **All employees**
Employees are the primary role-players in the process of complying with regulatory requirements. Their specific responsibility is to be conversant with, and to implement the specific requirements promulgated by the relevant Regulators.

(i) **Regulators**
The role played by the Regulator naturally depends on the specific business and the environment in which it functions. In general, the main objective of the Regulators is to maintain stability in the specific environment by providing guidelines and ensuring compliance therewith. Regular interactions between the specific Regulator and the aforementioned role-players are imperative in order to enhance a mutual understanding of the different perspectives on compliance matters.

2.2 **King II**
The King Report on Corporate Governance for South Africa (also known as King II) was first published in March 2002. As a result this report, a Code of Corporate Practices and Conduct was drawn up. It is referred to as the 'King Code'. The ‘King Code’, is structured under the following headings:
- Boards and directors
- Risk management
- Internal audit
- Integrated sustainability reporting
- Accounting and auditing
- Compliance and enforcement

Each of the above, either directly or indirectly, addresses different aspects of compliance.

2.3 **Conclusion**
Compliance is about more than just manuals, checklists and procedures. The extent to which the importance of compliance is correctly perceived will depend on the effectiveness of the interaction between the different role-players described above. This can only be achieved if each role-player fully understands their individual roles (mandate), as set out in this Section.
## APPENDIX 1

<table>
<thead>
<tr>
<th>Role-Players</th>
<th>Compliance considerations</th>
</tr>
</thead>
</table>
| **Board of Directors**  
The Board is appointed by and accountable to the shareholders, to lead, control and monitor the business and to provide effective corporate governance. | The Board is ultimately accountable for compliance and has the specific responsibility to oversee compliance with regulatory requirements. |
| **Audit/Compliance/Risk Committee**  
These sub-committees of the Board must be established to oversee various compliance matters. | The Audit/Compliance/Risk committee's monitors compliance at the highest level. The compliance officer typically has a reporting line to these committees. |
| **Executive Management Committee**  
The Executive Management committee is appointed by the Board to oversee and manage the business within an acceptable risk profile and to achieve sustainable profits. | The Executive Management committee is specifically responsible for ensuring that risk processes, including compliance with regulatory requirements, are implemented. |
| **Line Management and/or Boards for Divisions and Subsidiaries**  
Line management and/or Boards for Divisions and Subsidiaries accept responsibility for the risks undertaken in their divisions and/or subsidiaries within the confines of the overall risk control framework. | Their specific responsibility regarding compliance includes the implementation of compliance procedures to ensure adherence to relevant regulatory requirements within their divisions and/or subsidiaries. |
| **All Employees**  
Employees are the primary role-players in the process of complying with regulatory requirements. | Each employee must be conversant with, and implement the specific requirements promulgated by the relevant Regulators, as reflected in the business's operating procedures. |
| **Internal Audit Function**  
There is common ground between the compliance and internal audit functions, although the respective focuses are different. The internal audit manager could review the work conducted by the compliance officer as part of his/her normal audit responsibility. A good and interactive working relationship between the audit and compliance functions should be maintained. | The role of internal audit is to review the existence and adequacy of management control systems to ensure proper compliance with laid down policies, plans, procedures and regulatory requirements. The compliance function can therefore, in certain instances, rely on work that was done by internal audit instead of carrying out compliance reviews on their own, while internal audit could consult with the compliance function in identifying high risk areas in the planning of audits. |
External Audit Function
The external auditors are required by statute to conduct an audit on the business on an annual basis. Auditors also provide other services.

The external auditors are required to review the risk processes as part of their statutory audit duties imposed on them by the Companies Act, Banks Act and other applicable legislation.
<table>
<thead>
<tr>
<th><strong>Regulators</strong></th>
<th>Regulators monitor and enforce compliance with the regulatory requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The role played by the regulator naturally depends on the specific business and the environment within which it functions, but in general the objectives of regulators include systemic stability, financial safety and soundness and <strong>consumer protection</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
3. THE REGULATORY ENVIRONMENT

3.1 Introduction

"Historically, financial regulation has emerged in the wake of financial scandal." Quote Andrew Newton

The actions of rogue trader Nick Leeson, an employee of Barings Bank, which ultimately led to the demise of the Bank, is a classic example of financial regulation emerging in the wake of a financial scandal. The facts of the demise of Barings Bank are as follows: Leeson, who was employed by Barings Bank, applied to register as a trader with the Securities and Future Authority (the U.K. regulator for the financial services industry) in London, but his application was turned down because he had misrepresented certain information. He then transferred to Singapore where he applied to the local regulator for registration. Not knowing that he had been turned down in London, Singapore registered Leeson as a trader.

Although Barings Bank had a compliance function; there was no proper separation of duties as well as ineffective and inadequate controls.

The following extract from the conclusion of the Bank of England Report on the Collapse of Barings (paragraph 13.13) provides an indication of the inadequate controls in Barings Bank:

"The fact that Leeson was permitted throughout to remain in charge of both front office and back office at BFS was a most serious failing. Witnesses whom we have interviewed on this point agreed that the need for a separation of responsibilities was fundamental. Tony Hawes, the Group Treasurer, had relatively early on (in February 1994) identified this as unsatisfactory. He subsequently made his views known to James Baker, prior to James Baker's internal audit of BFS undertaken in July/August 1994. Although the internal audit did not unearth the existence of the unauthorized activities, the internal audit report did make specific recommendations as to the separation of roles. These recommendations were never implemented".

The Bank of England Report (paragraph 13.11) also provides an indication of where the responsibility for the inadequate controls in the Bank lay:

"We consider that those with direct executive responsibility for establishing effective controls must bear much of the blame. We identify below the ways in which, we have concluded, they failed to discharge this responsibility; and how others at lower levels of management were also at fault for failing to act effectively in relation to their own responsibilities".

The collapse of the bank resulted in significant changes to the way in which the regulatory authorities were structured and in the regulatory requirements themselves.

"The Economic Secretary for the United Kingdom, Ms Helen Liddell, has recently stated that she fails "to see the difference between over-trading and theft, between trading on your own account to your client’s disadvantage and theft and between deceiving clients to profit from their loss and theft." Page 18, Newton.

Other examples of financial scandals include the collapse of the banking systems in many of the Southeast Asian countries. These Countries suffered severe economic
difficulties, which significantly impacted on their people. As a result, they now support tougher regulation.

In South Africa, we have seen the collapse of Beige (a pharmaceutical company), Leisurenet and Saambou Bank in recent years.

3.2 The philosophy and objectives of regulation

One of the primary functions of Government is to ensure the nation's economic well-being. To achieve this, Government must make sure that South Africa remains an attractive capital market for investors and consumers.

To quote Gill Marcus, at the time Chairperson of the Policy Board for Financial Services and Regulation: "The importance of designing and maintaining an efficient and effective system to regulate financial markets, financial institutions and financial services lies at the very core of our nation's well being" Foreword to Financial Regulation in South Africa

The role of Government, Regulators and other authorities is to:
- Maintain confidence in the financial system; and
- Protect the interests of consumers.

Each of these aspects will be discussed in more detail:

(a) Maintain confidence in the financial system — Prudential regulation

In order to successfully attract business to the South Africa financial markets, investors, depositors and customers must have confidence that the financial service providers that they are dealing with are financially sound and that they will act with integrity. Government must guard against the risk that the whole financial system could be impaired by the insolvency of a single financial services provider.

An example of regulation that aims to maintain confidence in the financial system is set out below:
- Capital adequacy requirements that serve as a cushion against operating losses. Businesses are required to keep adequate capital to ensure financial soundness.

This type of regulation is known as prudential regulation.

(b) Protect the interests of consumers — Consumer protection regulation

Financial and investment products can be complicated, making it difficult for consumers to understand them and to assess their value, soundness and risk.

Government seeks to ensure that financial service providers rectify this knowledge imbalance and thereby level the playing fields. Government does this by regulating the industry.

The FAIS Act is an example of regulation that aims to protect consumers. The requirements of the Act stipulate that:
- Persons who sell financial and investment products are "fit and proper"; and
- They adequately disclose certain information relevant to the transaction to the client.
This type of regulation is known as "consumer protection regulation" or "market conduct regulation".

3.3 Regulatory requirements
From the philosophy and objectives of regulation we see that government aims to regulate the financial services industry to maintain confidence in the financial system and to protect consumers. The Government and other authorities achieve this through the enacting of laws.

Explanation:

Definition
"Regulatory requirements" is the term that is used to collectively describe the requirements set out in:

- Acts of Parliament (e.g. the FIC Act)
- Subordinate legislation, (e.g. the regulations to the FIC Act), and
- Supervisory requirements (e.g. guidance notes issued by regulators)

There is no doubt that, on a daily basis, there are more and more regulatory requirements with which compliance officers must comply. Some examples are:

- The Financial Advisory and Intermediary Services Act (FAIS), which specifies that the rendering of financial advice or intermediary services in relation to financial products is done in a competent and open manner;
- The Financial Intelligence Centre Act (FIC), which requires that any suspicions relating to unlawful activity must be reported to the Financial Intelligence Centre.

Although compliance with regulatory requirements represents a significant challenge, the purpose is not to frustrate business activity. The aim is to support the development of business while protecting investors, depositors and consumers.

In the final analysis, compliance is simply "good business". Much of what is included in the regulatory requirements represents good business practice. For example, FAIS contains requirements that will result in good client service, if applied appropriately. Businesses that have effective compliance functions will usually be seen in a positive light by stakeholders, which in turn will protect or enhance their reputation.

However, with the ever-increasing volume and complexity of the regulatory requirements, it is important to address the cost of compliance. The impact of these requirements is becoming more and more onerous and, accordingly, more costly. For example, training challenges relating to a number of high impact regulatory developments require ongoing expenditure.

All financial service providers who wish to operate a long-term sustainable business must successfully manage compliance with regard to the applicable regulatory requirements!
3.4 Regulators

Regulators are appointed to promote/enforce adherence to these regulatory requirements. These regulators are created and derive their power from certain pieces of legislation.

The two main financial services industry regulators are:

- The South African Reserve Bank (SARB) — created in terms of the South African Reserve Bank Act/the Banks Act; and
- The Financial Services Board (FSB) — created in terms of the Financial Services Board Act.

These Acts make it illegal to conduct a specific type of business unless the financial service provider is authorised or licensed to conduct such business. The financial service provider is required to undergo a process of licensing and to enter into a relationship with the regulator in terms of which the financial services provider undertakes to comply with the regulatory requirements.

3.5 Management of the regulatory requirements

Compliance with regulatory requirements is one of the most significant challenges facing management today.

The regulatory requirements set minimum standards, for example:

- Minimum capital adequacy requirements/maintaining sufficient levels of financial resources;
- Ensuring that individuals who are hired are adequately trained to do the jobs they do;
- Minimum disclosure of information;
- Controlling advertisements;
- Minimum standards for handling monies received from clients;
- Establishing "fit and proper" requirements; and
- Prohibiting insider training.

The regulatory requirements also stipulate that any licensed financial services provider report must complete an annual compliance report for the regulator. The purpose of this report is to enable the regulator to monitor compliance with the legislation.

3.6 Impact of non-compliance on business

As already mentioned, compliance with regulatory requirements is a complex challenge. The number of requirements is already large and growing. Part of the challenge is the difficulty inherent in interpreting the requirements. Furthermore, the requirements are often applied in a varied manner from business to business.

The legislation mandating a regulator will set out that regulator's powers, which include the power to take disciplinary action. Such disciplinary action could be in the form of:

- The imposition of fines.
- The publication of details of the misconduct in the public domain.
- The de-registering or suspending of a financial services provider.
However, not only do business owners need to concern themselves with the perception of the regulator with regard to the manner in which the business is conducted, but business owners must also take into account the perceptions of clients and investors with regard to how they conduct business.

3.7 International trends
South Africa operates within the global arena. As international financial service providers are transacting with South African financial service providers on a daily basis, they expect the South African market to be financially sound. This will be determined, to a large extent, by monitoring the level of prudential supervision that the financial service providers are subjected to. If South Africa wishes to continue to be a global player, the country must meet and maintain the standards that are set internationally.

As is the case locally, the intensity of regulation is also increasing internationally. Financial service providers that fail to adapt to the regulatory environment will be subject to increasingly severe disciplinary action.

The UK and USA supervisory regimes have embraced an increasing focus on the supervision of money laundering control requirements. This trend is also being adopted in South Africa. (Take note: The supervisory role that is played by the Financial Intelligence Centre, the Reserve Bank, and/or the Financial Services Board, regarding money laundering control is beyond the scope of this Manual).

3.8 Legislation
The table below provides an overview of some of the legislation that has been put in place with regard to the differing types of businesses.

<table>
<thead>
<tr>
<th>Acts</th>
<th>Regulator</th>
<th>Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks Act</td>
<td>Registrar of Banks</td>
<td>Banks</td>
</tr>
<tr>
<td>Long Term Insurance Act &amp; Policy Holder Protection Rules</td>
<td>Registrar of Long Term Insurance (FSB)</td>
<td>Long-Term Insurers</td>
</tr>
<tr>
<td>Short Term Insurance Act</td>
<td>Registrar of Short Term Insurance (FSB)</td>
<td>Short-Term Insurers</td>
</tr>
<tr>
<td>Pension Funds Act</td>
<td>Registrar of Pension Funds (FSB)</td>
<td>Pension Funds</td>
</tr>
<tr>
<td>Collective Investment Schemes Act</td>
<td>Registrar of Collective Investment Schemes (FSB)</td>
<td>Investment Schemes</td>
</tr>
<tr>
<td>Financial Intelligence</td>
<td>Financial Intelligence Centre</td>
<td>Accountable Institutions</td>
</tr>
</tbody>
</table>
3.9 Stakeholders
The following diagram graphically represents the stakeholders within the regulatory environment.

<table>
<thead>
<tr>
<th>Centre Act</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial Advisory and Intermediary Services Act</strong></td>
<td>FSB, FATS Ombud</td>
</tr>
</tbody>
</table>

**GRAPHIC REPRESENTATION**
**OF THE REGULATORY ENVIRONMENT**

**GOVERNMENT**

**REGULATORS**

**CONSUMERS**

**INVESTORS**

**DEPOSITORS**

**Acts of Parliament**

**Subordinate legislation**
Government is tasked with ensuring our nation's economic well-being and enacts legislation to regulate the financial services industry.

Regulation takes the form of prudential supervision and/or consumer protection regulation in order to protect the rights and interests of investors and consumers.

Regulators are established in terms of the legislation and empowered to monitor and ensure adherence to the regulatory requirements. These
regulators may issue supervisory requirements with which one must comply.
SECTION 3

Financial services providers must structure the way in which they conduct business to meet the minimum standards set out in the regulatory requirements.

The Board of Directors is ultimately responsible for compliance. This task is delegated to senior management. Management may appoint compliance officer to assist it in complying with the regulatory requirements.

The regulatory requirements impact on business transactions making it necessary for all employees employed by a financial services provider to play their part in ensuring compliance with the regulatory requirements.

3.10 Conclusion

Whether as a result of international trends or pressure from stakeholders, the intensity of regulation is increasing. Managing compliance with these regulatory requirements will remain a significant challenge to management.
As indicated in the diagram, the South African Reserve Bank regulates banks while other financial services institutions are regulated by the FSB.
4. ROLE OF THE REGULATORS

4.1 The regulators in the context of the financial services industry
In order to provide an understanding of the role played by the respective regulators, their mission statements, as published on their websites (February 2004), are reflected below.

_The South African Reserve Bank (SARB)_
"The Reserve Bank is responsible for bank regulation and supervision in South Africa. The purpose is to achieve a sound, efficient banking system in the interest of the depositors of banks and the economy as a whole. This function is performed by issuing banking licences to banking institutions, and monitoring their activities in terms of either the Banks Act (No. 94 of 1990), or the Mutual Banks Act (No. 124 of 1993)."
[www.resbank.co.za](http://www.resbank.co.za)

_The Financial Services Board (FSB)_
"The Financial Services Board is a unique independent institution established by statute to oversee the South African Non-Banking Financial Services Industry in the public interest. Our mission is to promote sound and efficient financial institutions and services together with mechanisms for investor protection in the markets we supervise."
[www.fsb.co.za](http://www.fsb.co.za)

The mandates of the above regulators are set out in the legislation that makes provision for the establishment of each particular regulator.

4.2 The role of a regulator
As can be seen from the above mission statements, one of the primary roles of a regulator is to licence financial institutions. It is interesting to note that on one hand the focus is on depositors whilst on the other hand, the focus is on investors.

Regulators also determine whether certain persons/financial services providers meet "fit and proper" requirements.

In order for regulators to discharge their responsibilities they require information. This can be obtained in a number of different ways. For example:

- Routine reports received from the businesses themselves, e.g., the "DI returns" which must be submitted by Banks to the Reserve Bank. These cover the financial position, income statement, liquidity, capital adequacy and other risks of the bank.
- On-site inspections conducted by the regulator.
- Information requested by the regulator on matters that the regulator may be investigating.
- Information or complaints received from customers and investors.

In broad terms, regulators enforce compliance with the regulatory requirements by taking disciplinary action against non-compliant businesses.

Regulators are, in effect, the custodians of the legislation that regulates the businesses for which they are responsible. The regulator must consider the appropriateness of the legislation and advise government on amendments which should be made thereto. Further, regulators consider international trends in regulation with a view to advising government on the way forward. The South African regulatory environment is continually evolving in line with international developments.
They may also issue appropriate guidance notes or directives to assist in the interpretation of regulatory requirements or to enhance the regulatory requirements.

4.3 South African Reserve Bank

The Reserve Bank's mission statement provides useful insights. The key aspects are:

- The purpose is to achieve a banking system which is:
  - Sound,
  - Efficient, and
- In the interest of:
  - The depositors of banks, and
  - The economy as a whole.
- This function is performed by:
  - Issuing banking licences to banking institutions, and
  - Monitoring their activities in terms of either the Banks Act, or the Mutual Banks Act.

In view of the need to promote a sound financial system, banks are regulated to ensure they are prudently managed. The Bank Supervision Department (BSD) of the SARB undertakes this function, the head of which is the Registrar of Banks. Although BSD forms part of the SARB, it operates somewhat independently from the SARB.

4.4 Financial Services Board

The key aspects of the Financial Services Board mission statement are set out below:

It is a unique independent institution established by statute to:
- Oversee the South African Non-Banking Financial Services Industry,
- In the public interest.

The FSB's mission, as reflected above, is to promote:
- Sound and efficient financial institutions and services, and
- Together with mechanisms for investor protection in the markets that it supervises.
5. HOW THE REGULATORS IMPACT ON BUSINESS

5.1 Introduction

Newton writes the following in his book, 'The Handbook on Compliance', on the role of the regulators in the United Kingdom:

"You need their continuing permission in order to conduct business. You are obliged to be open and co-operative with them. They can ask you for almost any information or documentation and they can inspect your business at any time with or without notice. If they do not like what they see your firm can be warned, fined, pilloried, ordered to pay compensation or have its profits redistributed among claimants. Ultimately, they can suspend or terminate your firm's authorization, and can prevent any individual from taking up or remaining in employment in the financial services industry in the United Kingdom and, practically speaking, in any major financial centre in the world. Neither you nor your firm can afford to incite them to action." Newton, Page 22.

5.2 Licensing or authorisation

In order to conduct the business of a bank, a banking licence must be obtained from the South African Reserve Bank. A bank cannot conduct business without this licence.

In order to obtain the relevant licence/authorisation, the business must make an application to the authority in question. One of the requirements of the application is that the business must establish that it is able to meet the minimum requirements that are set out with regard to the 'fit and proper' requirements in the legislation.

There is an ongoing requirement in this regard. At any time after obtaining the licence/authorisation to conduct business, the regulator may withdraw the licence/authority to conduct business if certain requirements are not being met. For example, for any registered bank, the SARB could withdraw their banking licence if the bank no longer complies with the relevant requirements.

5.3 Business implications

The minimum standards are set out in the regulatory requirements. There is an expectation on the part of the Regulators that the manner in which business is conducted, is adjusted in order to meet these minimum standards.

For example, the FICA requires that accountable institutions "identify" and "verify" their clients. This means that all account opening procedures must be adjusted to ensure compliance.

Businesses that fall within the definition of "accountable institutions" are specified in Schedule 1 of the Financial Intelligence Centre Act. Some examples include:

- Banks
- Attorneys
- Estate agents
- Any "long-term insurance business"
- Members of a stock exchange, etc
The above list is by no means complete and is included for illustration purposes only.

**5.4 Compliance management system**

As discussed earlier, many of the regulatory requirements must be integrated into business processes and thereafter managed. What makes it even more challenging is that there are new regulatory requirements being issued and existing ones are being amended on a continual basis!

Regulators expect that a business will implement a system to manage these regulatory requirements.

For example, the Financial Intelligence Centre Act (see Section 43 of the Act) requires that a financial services provider appoint a compliance officer to be responsible for compliance with the regulatory requirements.

Most large organisations have employed compliance officers in their head-offices, as well as in their business units, to assist senior management in implementing compliance risk management systems.

**5.5 Reporting**

In order to monitor compliance with the regulatory requirements, the Regulators require business to report on compliance with specific regulatory requirements within specified timeframes, for example on a monthly, quarterly or annual basis.

An example of this is the "DI Returns" that are submitted to the Bank Supervision Department of the SARB. In these DI Returns, senior management of the financial services providers are required to confirm by signature that, for example:

- The bank holds sufficient capital; and
- The bank is complying with the money laundering control requirements.

Another example is the requirement in terms of sec 17(4) of the FAIS Act that annual compliance reports be submitted to the FSB.

**5.6 Complaints handling**

Regulators also handle complaints that are lodged with them in respect of the businesses that are licensed by them. The complaints are received by the Regulator and his staff, investigated and then resolved.

This complaints resolution process requires interaction between the business and the Regulator.

**5.7 Monitoring**

Regulators are tasked with monitoring compliance with regulatory requirements. Methods to monitor compliance that are imposed on a business include:

- Reporting (as discussed above).
- Complaints handling (as discussed above).
- Requests for information directly from the business:
  - The regulator has the power to request any information from the business in respect of compliance with a regulatory requirement.
- On site investigations:
  - The regulator has the authority to conduct an on-site investigation in respect of compliance with the regulatory requirements. Such on-site investigations can take anything from a few days to a couple of weeks to complete.
5.8 Disciplinary action

The Regulators are also required to enforce compliance with the regulatory requirements by taking disciplinary action against "non-compliant" businesses. Disciplinary action can, depending on the legislation, take the form of:

- The imposition of a fine.
- The imposition of supervisory sanctions.
- The publication of details of the misconduct in the public domain.
- De-registering or suspending the offending person or business.

**SOCCER**
- The playing field
- The ball
- The points score
- The player/teams
- The referee

**REGULATORY ANALOGY**
- The financial services market
- Financial instruments and products
- Money
- Business
- The regulator with the power to enforce the rules of the game and discipline the players
- The regulatory requirements

5.9 Conclusion

Regulators impact on business in the following respects:

- The relevant licensing requirements of different businesses;
- Monitoring compliance with regulatory requirements, through reporting, investigations and complaints handling; and
- Enforcing compliance with regulatory requirements through disciplinary action.

Regulators also require that businesses:

- Adjusts the manner in which they conduct business to comply with regulatory requirements; and
- Institute compliance management systems as required by the relevant legislation.
6. COMPLIANCE OBJECTIVES

6.1 Introduction

This section sets out the main objectives of the Compliance Function and specifies the role of the Compliance Officer.

6.2 Objectives of the Compliance Function

The objectives of the Compliance Function, as part of an effective risk management framework, include the following:

(a) To assist line management in discharging its responsibility to comply with applicable statutory, regulatory and supervisory requirements;
(b) To enable the company to demonstrate to the Regulators that it is fit and proper to undertake its business;
(c) To facilitate the management of Compliance Risks;
(d) To avoid disciplinary action by Regulators;
(e) To minimise the possibility of civil and criminal action against the company.

6.3 Role of a Compliance Officer

The primary role of the Compliance Officer is to facilitate the effective management of the compliance risk by the subsidiaries and divisions through, inter alia, the following:

(a) Setting organisation wide policy and standards for compliance;
(b) Providing advice on compliance related matters;
(c) Compiling of a compliance manual with sufficient references to relevant operational manuals;
(d) Establishing and maintaining a compliance culture, in conjunction with line management, within the company which contributes to the overall objective of prudent risk management of the company;
(e) Monitoring the level of compliance on an ongoing basis;
(f) Establishing and maintain working relationships with relevant stakeholders;
(g) Providing assistance to minimise the damage to the company’s reputation/image in cases where material transgressions occur;
(h) Promoting a compliance culture through effective training programmes and compliance awareness campaigns;
(i) Report to board, audit committee, line management and regulators; and
(j) Attend to recommendations from board, audit committee, line management and regulators.

6.4 Conclusion

In striving to achieve these objectives the Compliance Officer should act proactively and constructively and assist line management in running an efficient and profitable business, without violating statutory, regulatory and supervisory requirements. Compliance Officers should also strive to gain the support of line management without jeopardising their independence.
7. COMPLIANCE STRUCTURES

7.1 Introduction
This section provides the reader with a perspective on the underlying principles that should be taken into consideration in determining an effective compliance structure.

7.2 Background
The fostering of a culture of compliance, as well as optimising relations with the relevant Regulators requires a multidisciplinary approach that can only be effective if all the relevant role-players actively support the compliance system and its objectives. Therefore it is imperative that the relations and communication channels between the different role-players are clearly set out in an appropriate structure. (A comprehensive list of the relevant role-players that are likely to be part of this process can be found in section 11 of this Handbook).

Although the format of the compliance system will differ from business to business, in order to implement an effective compliance system, it must be based on the principles as set out in Regulation 47 of the Banks Act No 94 of 1990. These principles require that any compliance system that is implemented enables the Compliance Officer to:
(a) Provide the Board of Directors with regular information as regards with the level of compliance to supervisory requirements;
(b) Function independently from other functions of internal control;
(c) Ensure that no conflict of interest exists with other internal control functions, for example, the Internal Audit Function;
(d) Report issues of non-compliance to the CEO and the Board of Directors in a timely manner;
(e) Have direct access to the Chief Executive Officer (CEO); and
(f) Have senior executive status in the business.

7.3 Suggested compliance structure
The compliance structure will usually depend on the geographical and/or key activities of the business. Therefore a large organisation with a number of widespread business units would warrant a more complex structure for compliance than a smaller business for which a simple structure is quite sufficient.

Large organisations may have a Compliance Officer for the holding company as well as Compliance Officers for the different business units and /or subsidiaries. Although the Compliance Officer for the holding company (Group Compliance Officer (GCO)) will take overall responsibility for compliance, the Compliance Officers in the business units and subsidiaries (Business Unit Compliance Officers (BCO)) will assist the GCO by taking on responsibility for compliance within their specific business units. In a smaller business that has a simpler compliance structure, the compliance function may be the responsibility of one person.
Take note of the following with regard to the compliance structure:
(a) Role-players in the compliance process with reference to their specific roles, authorities and responsibilities (refer to Section 11 of the Handbook);
(b) Interaction with other role-players (refer to Section 2 of the Handbook);
(c) Reporting lines (refer to section 6 of the Handbook);
(d) Details of responsible contact persons; and
(e) The positioning of the Compliance Function within the bigger risk management framework.

7.4 Conclusion
The most important criterion for an effective compliance structure is that it must provide the Compliance Officer with easy access to the CEO and Board of Directors in order for him/her to discharge reporting duties independently, efficiently and effectively.
8. THE COMPLIANCE FUNCTION

8.1 Introduction
The compliance function plays an invaluable role in any business. It is relied on to assist the business in complying with the ever-increasing obligation of regulatory requirements. This is driven, on the one hand, by regulatory requirements that demand compliance and, on the other hand, by business imperatives that recognise that compliance is simply good business practice.

Sound corporate governance is essential for effective compliance.

8.2 Scope of the Compliance Function
In terms of Regulation 47 of the Banks Act No 94 of 1990 (Regulation 47), a bank must establish an independent compliance function as part of its risk management framework in order to ensure that the bank continuously manage its regulatory risk.

The responsibility for monitoring compliance risk is normally delegated to the Head of the Compliance Function (Compliance Officer).

Compliance risk is the risk that the procedures implemented by the business to ensure compliance to relevant statutory, regulatory and supervisory requirements are not adhered to and/or are inefficient and ineffective. Compliance risk consists of both a regulatory and reputational element:

Regulatory risk is the risk that a business does not comply with regulatory requirements or excludes provisions of relevant regulatory requirements from its operational procedures.

Reputational risk is the risk that the business might be exposed to negative publicity due to the contravention of applicable regulatory requirements.

According to Regulation 47, the scope of a financial institution's compliance function comprises of all the statutory, regulatory and supervisory requirements that fall within the ambit of the compliance risk. The recommended approach is to be inclusive rather than exclusive in determining the scope for the compliance function. This implies that formal internal policies, procedures and business practices should also fall within the scope of the compliance function. (Given the role normally played by the Internal Audit Function with regard to internal controls, it is imperative for the Compliance Function to liaise closely with Internal Audit in order to avoid duplication and inefficiencies).

The scope of the Compliance Function may therefore include requirements that are already monitored by other functions. An example of this situation would be the employment equity aspects by the Human Resource function or computer software licence and copyright matters by the Information Technology function.

Given the various potential role-players in the compliance function, a well-defined and documented "scope" is imperative for managing the Compliance Function effectively.

The scope of the Compliance Officer function must not be defined too narrowly, as this may result in the compliance risk being unacceptably high.
8.3 Responsibility for Compliance

The Board of Directors is ultimately accountable for compliance with the regulatory requirements that are imposed. The governance structures will, of necessity, address the delegation of responsibility to management and employees.

At the outset, it is important to note that the compliance function is not ultimately responsible for compliance. The compliance function's key contribution is to "assist management in discharging their responsibility to comply with regulatory requirements".

It is clear that making compliance officers responsible for compliance would be as ill-advised as:

- Making internal auditors responsible for internal controls; or
- Making risk managers responsible for operational risks.

As previously mentioned, ultimately management is responsible for conducting business in compliance with applicable regulatory requirements. The compliance officer's role is to assist management to achieve this.

8.4 Compliance Officers

The King II Report provides guidelines on what the role of the compliance officer encompasses:

- Providing a service to management by assisting them in identifying and prioritising all applicable regulatory requirements;
- Providing awareness training to enable management to manage applicable compliance risks appropriately; and
- Conducting monitoring programs to identify and report aspects of non-compliance to the CEO and Board.

Although this is a high-level description, it cuts to the core of the contribution that is made by compliance officers. The King II Report also states that:

'The primary role of the compliance officer is to assist management in discharging its responsibility to comply with statutory, regulatory and supervisory requirements by facilitating the development, establishment and maintenance of an efficient and effective compliance risk management process'.

The above statement is also supported by King II guidelines relating to risk management structures. Specifically, the following is stated:

"Although management may appoint a chief risk officer or risk facilitator to assist in the execution of the risk management process, the accountability to the board remains with management and should be the responsibility of every employee".

This theme is emphasised in section 60A of the Banks Act that states that:
(1) Notwithstanding anything to the contrary in any law, a bank shall establish an independent compliance function as part of the risk management framework of the bank.
(2) The compliance function shall be headed by a compliance officer of the bank, who shall perform his or her functions with such care and skill as can reasonably be expected from a person responsible for such a function in a similar institution.

(3) The appointed compliance officer shall perform his or her functions subject to such requirements and conditions as may be prescribed in the regulations relating to Banks.

Regulation 47 of the Banks Act specifies a number of requirements that underpin the risk management approach that is encouraged by the Bank Supervision Department of the South African Reserve Bank:

Although the FAIS Act does not recognise the compliance "risk role" to the same extent as the Banks Act, it specifies that each financial services provider (with more than one key individual or representative) must appoint a compliance officer and establish compliance procedures to be followed by it and its representatives.

It is noted that, to a large extent, the FAIS Act's focus is on monitoring. For instance, compliance officers are required to submit a compliance report to the Registrar of Financial Services Providers. This report is, in essence, a "checklist" covering key compliance matters.

The specifications contained in the likes of the King II report and certain regulatory requirements (such as regulation 47) are considered to be in line with international practice.

Compliance is most effective when integrated into business processes. It should not be seen in isolation and should be seen in the light of various related role-players.
9. DUTIES AND OBLIGATIONS OF THE COMPLIANCE OFFICER

9.1 Introduction
The first step in meeting the compliance challenge lies in setting up an appropriate compliance structure and appointing a compliance officer to assist management in complying with the regulatory requirements.

Every employee must also be trained in respect of the regulatory requirements that impact upon his/her job and they must assume responsibility for compliance with such regulatory requirements. Further, it is in the interests of the employee to ensure that he/she effectively manages compliance, as it should be included as an important aspect of a performance assessment.

9.2 Who is responsible for compliance?
Before considering the duties and obligations of the compliance officer, it is important to ascertain where the ultimate responsibility for compliance lies.

"The Compliance function exists, not to take responsibility for ensuring that a firm fulfils its regulatory obligations, but to assist the management of the business in its responsibility to comply with the regulations." Newton, page 92.

9.3 Accountability of Directors versus Responsibilities of Compliance Officers
The responsibility for managing the entity's business rests with the Board of Directors and CEO of each business unit. Accordingly, the management of each business unit is responsible for compliance to statutory, regulatory and supervisory requirements and is liable for the consequences of non-compliance. The Board and CEO delegate authority to the Compliance Officer to ensure that the compliance process is running effectively and that statutory, regulatory and supervisory requirements are adhered to. The Board and CEO are, however, ultimately accountable for compliance.

9.4 Responsibilities of the Compliance Officer
The responsibilities of the Compliance Officer will differ from entity to entity and it could even differ within an entity, depending on the position of the appointed compliance officer in the entity. In general it can be expected that a Group Compliance Officer's responsibilities will be more comprehensive than those of a Compliance Officer for a Business Unit and/or Region.

The following are examples of the most basic responsibilities that should be included in a job description of a Group Compliance Officer.

The Group Compliance Officer (GCO) is normally the person who takes on the overall responsibility for compliance for the Group and all its Strategic Business Units. The GCO has to work closely with the Group Chief Executive and the specific responsibilities include, *inter alia*, to:

8.4.1 **ensure compliance** within the group or entity in line with current laws, regulations and supervisory requirements or provisions;

8.4.2 **report non-compliance** to laws and regulations or supervisory requirements to the chief executive officer, the board of directors and the audit committee in a timely manner;

8.4.3 **provide** the board of directors and the audit committee with regular reports as regards the level of compliance by the entity to laws and regulations or supervisory requirements;
9.4.5 **ensure**, as far as possible, that no conflict of interest with/between other internal control functions exists;

9.4.6 **establish a compliance culture** in the entity that contributes to the overall objective of prudent risk management by the entity;

9.4.7 **establish a line of communication** to line management in order to continuously monitor compliance by the entity to laws and regulations or supervisory requirements;

9.4.8 **require of line management to monitor compliance** with laws and regulations or supervisory requirements as part of their normal operational duties;

9.4.9 require **regulatory requirements to be incorporated** into operational procedures manuals where appropriate;

9.4.10 **make recommendations** whenever necessary to ensure that laws and regulations or supervisory requirements are being complied with;

9.4.11 **establish prompt mechanisms for reporting** and resolving non-compliance to laws and regulations or supervisory requirements;

9.4.12 ensure that **resolutions are signed off**;

9.4.13 **document his / her findings**, including any remedial action, as part of the compliance monitoring programme;

9.4.14 **recruit sufficient staff** of the correct quality in order to continuously monitor and test the entity's compliance to laws and regulations or supervisory requirements;

9.4.15 **ensure that compliance staff are trained** on a continuous basis in order to ensure that they have adequate technical knowledge in order to understand the regulatory framework that applies to the entity as well as the risks to which the entity is exposed to; and

9.4.16 **compile and maintain a comprehensive compliance manual** for the Group.

*(Adopted: Regulation 47 of the Banks Act 94 of 1990)*

The Board and CEO is accountable for ensuring that the entity complies with all applicable laws, regulations and supervisory requirements but they will rely on the Compliance Officer to assist them in discharging that accountability. Responsibilities for Compliance Officers can never be prescriptive, but the aforementioned responsibilities or at least elements thereof should be present in all job descriptions/Key Performance Areas (KPA's) for Compliance Officers.

### 9.5 The formal duties and obligations of the compliance officer

The appointment of a compliance officer and the formal duties and obligations of the compliance officer are prescribed by law. Some examples are:

- Section 60/regulation 47 of the Banks Act
- Section 17 of the FAIS Act
- Section 43 of the FIC Act

Each of these requirements will be discussed in more detail:

**(a) Regulation 47 (Banks Act)**

The main objective of Regulation 47 is to support good corporate governance and effective compliance.

Regulation 47(1) of the Banks Act prescribes that a bank shall establish an independent compliance function as part of its risk management framework, in order to ensure that the Bank continuously manages its regulatory risk.
Definition:
Regulatory risk is the risk that the bank does not comply with the applicable regulatory requirements.

Regulation 47(2) provides that the compliance function shall be headed by a **compliance officer** of the bank, who shall perform the compliance officer's functions with diligence and care and with such a degree of competence as can reasonably be expected from a person responsible for such a function.

Regulation 47(3) provides that the compliance function shall have **adequate resources and stature** to ensure that non-compliance with laws and regulations or supervisory requirements by the bank can be addressed adequately.

Regulation 47(4) specifies **specific responsibilities** of the compliance officer. These fall under the following headings:
- Effectiveness
- Monitoring
- Reporting
- Resources
- Manual

It is noted that the requirements that are contained in Regulation 47 are considered to be in line with international best practice.

(b) Section 17 (FAIS Act)
The FAIS Act introduces requirements that are designed to promote compliance functions.

Section 17(1) of the Act specifies that any authorised financial services provider (with more than one key individual or one or more representatives) must, **appoint one or more compliance officers** to monitor compliance with this Act.

It is interesting to note that the abovementioned section narrowly defines the role played by compliance officers; namely, there is a predominant focus on monitoring. Whilst this is necessary, there is a concern that this section is incomplete by only focussing on one of the key compliance functions.

Section 17(1), read in conjunction with section 19(5), specifies that if the appointment of a compliance officer of an authorised financial services provider is **terminated**, the compliance officer must submit to the Registrar of Financial Services Providers a **statement** of what the compliance officer believes to be the reasons for the termination. The requirements relating to compliance reporting to the Registrar are also specified.

Section 17(2) specifies that a compliance officer must be **approved** by the registrar in accordance with the criteria and guidelines determined by the Advisory Committee. The Registrar is empowered to terminate the appointment of a compliance officer if approval requirements are no longer met, subject to the specified notice requirements.
Section 17(3) specifies that an authorised financial services provider must establish and maintain procedures to be followed by the provider and any representative concerned, in order to ensure compliance with this Act.

Section 17(4) specifies that a compliance officer or, in the absence of such officer, the authorised financial services provider concerned, must submit reports to the registrar in the specified manner.

For ease of reference the requirements of section 17 of the FAIS Act are detailed in Section 10.

(c) Section 42 and 43 of FICA

A further example of regulatory requirements relating to compliance officers is contained in section 43(b) of FICA. This section requires an accountable institution to appoint a person with the responsibility of ensuring compliance by:
- The employees of the accountable institution with the provisions of this Act and the internal rules applicable to them; and
- The accountable institution with its obligations under this Act.

Section 42 sets out the internal rules that must be formulated and implemented to comply with the Act and requires that these rules be made available to all employees.

Section 43(a) states that an accountable institution must provide training to all its employees to enable them to comply with the provisions of the Act and the internal rules applicable to them.

9.6 Functions and responsibilities of a compliance officer

The main functions and responsibilities of a compliance officer fall under three headings:
- Services
- Training
- Monitoring

These functions are in line with the recommendations that are contained in the King II Report.

The functions and responsibilities of a compliance officer are considered below:

(a) Services

(i) Providing advice on regulatory requirements

One of the core functions of the compliance officer is advising management on the regulatory requirements applicable to the business conducted.

The compliance officer must assist the business to:
- Identify the regulatory requirements applicable to the business;
- Analyse and understand the regulatory requirements; and
- Prioritise the regulatory requirements.

The compliance officer should also keep abreast of all changes to legislation and advise management of any new regulatory requirements.
requirements.
(ii) **Oversee implementation of compliance procedures**

The compliance officer should assist management in:
- Identifying control measures that will ensure compliance with the regulatory requirements; and
- The implementation of these control measures.

(iii) **Reporting**

The compliance officer must keep the Board of Directors and management informed of the level of compliance being achieved. This is undertaken, for example, through compliance reports that are submitted to the respective stakeholders on a regular basis.

(iv) **Contact with regulators**

The first point of contact for the Regulator is normally the compliance officer. The compliance officer should be available to resolve any regulatory issues that may arise. The regulators expect issues to be dealt with promptly and thoroughly.

The compliance officer also plays a valuable role in reporting compliance issues to the regulator. For example:
- Regulation 47 of the Banks Act requires that the compliance officer provide a copy of Board reports to the regulator; and
- Section 17(4) of the FAIS Act specifies that a compliance officer or, in the absence of such officer, the authorised financial services provider concerned, must submit reports to the registrar.

(b) **Training**

The compliance officer assists in developing a compliance culture. All employees should be encouraged to not merely comply with the rules, but to rather adopt a values-based system whereby they embrace the objectives underlying the regulatory requirements. This can be achieved through appropriate training.

The compliance officer should see to it that the compliance issues are integrated into the training received by an employee in respect of his/her responsibilities.

It is noted that the compliance officer need not deliver the training. This could be done by the training department or by external training providers. The compliance function will, however, play a key role in coordinating the efforts to train staff members. The compliance officer is often expected to play a "train the trainer" role in rolling out compliance training to staff members.

(c) **Monitoring**

Compliance monitoring is undertaken in order to evaluate whether business is conducted in compliance with regulatory requirements. This can be achieved through routine/ongoing monitoring procedures, or through the application of specific monitoring techniques, e.g. adequacy, consistency or substantive reviews.

The results of these monitoring exercises must be reported to management. Ideally, it is recommended that management or staff members themselves should conduct the majority of compliance monitoring.
9.7 Conclusion
On the one hand, the compliance officer assists management to comply with regulatory requirements, including producing solutions to compliance challenges faced by management. On the other hand he/she must remain sufficiently independent to be able to discharge his/her obligations.

The quote below illustrates the challenges facing the compliance officer today.
"Compliance professionals are often a focal point for the conflict and frustration which regulation can generate. Every day they are called upon to use their professional judgment to identify ways of achieving the objectives behind the regulations without producing unnecessary restriction on the activities of their employers, or incurring any undue commitment of resources". Newton, Page xiv.
APPENDIX 3

BANKING COMPLIANCE RESPONSIBILITIES

Regulation 47
Regulation 47(4) sets out the responsibilities of the compliance officer and provides that, as a minimum, the compliance officer of a bank shall-

Effectiveness
(a) Have **senior executive status** in the bank;
(b) Have **direct access** to and demonstrable support from the chief executive officer of the bank;
(c) Function **independently** from functions such as internal audit and shall be demonstrably independent;
(d) **Report non-compliance** with laws and regulations or supervisory requirements to the chief executive officer, the board of directors and the audit committee of the bank in a timely manner;
(e) Submit a **report on the level of compliance** with laws and regulations or supervisory requirements by the bank at every meeting of the board of directors or the audit committee of the bank and provide the Registrar with a copy of such a report; and
(f) Ensure, as far as possible, that **no conflict of interest** with/between other internal control functions exists.

Monitoring
(g) Be responsible for establishing a **compliance culture** in the bank that contributes to the overall objective of prudent risk management by the bank;
(h) Establish a **line of communication to line management**, in order to monitor continuously compliance with laws and regulations or supervisory requirements by the bank;
(i) **Require line management to monitor compliance** with laws and regulations or supervisory requirements as part of their normal operational duties;
(j) Require regulatory requirements to be incorporated into **operational procedure manuals** when appropriate; and
(k) Make recommendations whenever necessary in order to ensure that there is compliance with laws and regulations or supervisory requirements.

Reporting
(l) Establish **prompt mechanisms for reporting** and resolving non-compliance with laws and regulations or supervisory requirements;
(m) Ensure that **resolutions are signed off**; and
(n) **Document the compliance officer's findings** including any remedial action, as part of the compliance-monitoring programme.

Resources
(o) Recruit **sufficient staff of suitable auality in order to monitor** and test continuously the bank's compliance with laws and regulations or supervisory requirements; and
(p) Ensure that **compliance staff are trained** on a continuous basis to ensure adequate technical knowledge of the regulatory framework that applies to the bank, as well as the risks to which the bank is exposed.
Manual

(q) Compile and maintain a compliance manual that:

(i) Adequately addresses all material risks to which the bank is exposed;
(ii) Adequately addresses all material objectives and aspects of applicable legislation;
(iii) Refers to specific legislation, rules and regulations when appropriate;
(iv) Is readily available to all relevant staff; and
(v) Is reviewed and updated at least once a year.
APPENDIX 4

FAIS COMPLIANCE RESPONSIBILITIES

Section 17
Section 17 of the FAIS Act sets out requirements/arrangements relating to compliance officers.

In terms of Section 17(1) -
(a) Any authorised financial services provider with more than one key individual or one or more representatives must, subject to section 35(1) (c), appoint one or more compliance officers to monitor compliance with this Act by the provider and such representative or representatives, particularly in accordance with the procedures contemplated in subsection (3), and to take responsibility for liaison with the registrar.
(b) Such person may be a director, member, auditor, trustee, principal officer, public officer or company secretary of any such provider, or any other person with suitable qualifications and experience determined by the registrar by notice in the Gazette, after consultation with the Advisory Committee.
(c) The provisions of section 19(5) and (6), relating to an auditor of an authorized financial services provider, apply mutatis mutandis to a compliance officer.

Section 19(5), as adapted to reflect a compliance perspective in terms of Section 17(1) (c), specifies that if the appointment of a compliance officer of an authorised financial services provider is terminated -
(a) The compliance officer must submit to the registrar a statement of what the compliance officer believes to be the reasons for that termination; and
(b) If the compliance officer would, but for that termination, have had reason to submit to the registrar a report contemplated in subsection (4), the compliance officer must submit such a report to the registrar.

Section 19(6), as adapted to reflect a compliance perspective in terms of Section 17(1) (c), provides that:
(a) The registrar may by notice require an authorised financial services provider to terminate the appointment of a compliance officer of that provider, if the compliance officer concerned no longer complies with the requirements considered when the compliance officer was approved by the registrar in terms of subsection (2) (a) or otherwise fails to comply with any provision of this section in a material manner.
(b) A notice contemplated in paragraph (a) takes effect on a date specified in such notice and may only be sent out after the registrar —
(i) Has given the authorised financial services provider and the compliance officer concerned the reasons why the notice is to be issued; and
(ii) Has given the authorised financial services provider and the compliance officer concerned a reasonable opportunity to be heard; and
(iii) Has considered any submissions made by or on behalf of the authorised financial services provider or the compliance officer concerned.

Section 17(2) specifies that a compliance officer must be approved, by the registrar in accordance with the criteria and guidelines determined by the Advisory Committee.

Section 17(3) specifies that an authorised financial services provider must establish and maintain procedures to be followed by the provider and any representative concerned, in order to ensure compliance with this Act.
Section 17(4) specifies that a compliance officer or, in the absence of such officer, the authorised financial services provider concerned, must submit reports to the registrar in the manner and regarding the matters, as from time to time determined by the registrar by notice in the Gazette for different categories of compliance officers, after consultation with the Advisory Committee.

Section 17(5) specifies that the provisions of subsections (3) and (4) apply mutatis mutandis to any authorised financial services provider who carries on a business with only one key individual or without any representative.
APPENDIX 5
FICA COMPLIANCE RESPONSIBILITIES

Section 42
(1) An accountable institution must formulate and implement internal rules concerning—
   (a) The establishment and verification of the identity of persons whom the institution must identify in terms of Part 1 of this Chapter;
   (b) The information of which record must be kept in terms of Part 2 of this Chapter;
   (c) The manner in which and place at which such records must be kept;
   (d) The steps to be taken to determine when a transaction is reportable to ensure the institution complies with its duties under this Act; and
   (e) Such other matters as may be prescribed.
(2) Internal rules must comply with the prescribed requirements.
(3) An accountable institution must make its internal rules available to each of its employees involved in transactions to which this Act applies.
(4) An accountable institution must, on request, make a copy of its internal rules available to—
   (a) The Centre; and
   (b) The supervisory body that performs regulatory or supervisory functions in respect of that accountable institution.

Section 43
An accountable institution must—
   (a) Provide training to its employees to enable them to comply with the provisions of this Act and the internal rules applicable to them;
   (b) Appoint a person with the responsibility to ensure compliance by—
       The employees of the accountable institution with the provisions of this Act and the internal rules applicable to them; and the accountable institution with its obligations under this Act.
10. COMPLIANCE MANUAL

10.1 Introduction
This section describes the requirements for and suggested content of a compliance manual. The various requirements in applicable legislation for the financial service industry will provide minimum standards with which a compliance manual must comply.

10.2 Background
The Compliance Officer should facilitate the compilation of a compliance manual (manual) for the business in conjunction with the relevant role-players described in Section 11 of this Handbook. The manual must be based on the standards and norms provided by the Compliance Institute of South Africa. The manual should not only be customised for the business and the specific environment in which it functions, but it should also endeavor to:
(a) Address all the risks that fall within the scope of the compliance function;
(b) Address all material objectives and aspects of applicable regulatory requirements;
(c) Refer to specific legislation, rules and regulations applicable to a specific business and, where appropriate also focus on the "spirit of the law";
(d) Be practical and easily understood to enhance implementation;
(e) Be readily available to all staff members; and
(f) Be reviewed and updated according to applicable legislation.

Given the complexity and often-diverse activities of the different business units within a large organisation, in most cases it will be necessary to compile separate compliance manuals for each business unit. The compilation of a compliance manual for a business unit is the responsibility of the Compliance Officer for the specific business unit. Furthermore, depending on the compliance policy, the manual must:
1. Be based on the compliance manual for the organisation; and
2. Should be compiled in consultation and, in conjunction, with the Group Compliance Officer.

Preparing and issuing a manual is an integral part of an effective compliance system. Compiling such a manual is normally a comprehensive process that includes:
(i) Thorough research on the applicable regulatory requirements and the impact thereof on the business;
(ii) Consultation with relevant external and internal role-players; and
(iii) Presentations to stakeholders to introduce the manual.

The manual on its own cannot and will never ensure effective compliance, but it serves as the basis for establishing an effective compliance culture.

10.3 Format
The manual is an area where "substance" is more important than format, because inaccuracies and errors will most certainly cause the manual to lose credibility with users. However, the format is important in so far as it determines the effectiveness with which users will implement the standards and comply with the norms contained therein. Use the following principles as guidelines when determining the format of a compliance manual:
(a) A very theoretical and complex format should be avoided;
(b) Language should be kept simple and in cases where more complex legal terms have to be used, explanations must be provided;

©Compliance Institute of South Africa
Handbook for Members
(c) The more diagrams and practical examples that are included, the easier it is for users to understand and implement the manual;
(d) An electronic version of the manual will not only enhance the regular updating of it, but will also make distribution more economical; and
(e) A standard format for the manual will enhance standardisation and consistency, as well as improve the effectiveness and efficiency of training in this regard.

10.4 Content
The format of the manual is likely to differ from business to business; however, it must contain at least the following elements:

(a) Introduction/Background information
The rationale behind the establishment of an independent compliance function should be explained in this section by setting out:
(i) Management's commitment to the fostering of a culture of compliance with relevant regulatory requirements (the following documents could be included: Letter of endorsement from the CEO, copy of the Board Decision in this regard, etc.).
(ii) The mandate of the compliance function (this should relate to management's commitment in this regard and should include information on, inter alia, definitions, policies, objectives, standards, norms and responsibilities).
(iii) The relevance and roles of external regulatory/supervisory bodies.

(b) Board Resolution
The Board Resolution is an essential starting point for the various compliance systems and indicates that the Directors understand their obligation under the relevant legislation and that they have taken the necessary steps in this regard.
Board resolutions will differ from business to business, but in general, the following elements should be identifiable in a resolution:
(i) A clear indication that the Compliance Policy, as set out in Section 10 is endorsed and approved by the Board;
(ii) A clear commitment to compliance with relevant regulatory requirements; and
(iii) An indication of the process through which instances of non-compliance will be reported to and dealt with by the Board.

The importance of a well-structured Board resolution can never be emphasised enough. The Board resolution provides the Compliance Officer with authority to implement the necessary compliance systems and facilitate corrective measures when necessary. More importantly, however, it illustrates commitment to an effective compliance system from top management level downwards.

(c) Compliance structures/function
This section should set out the following aspects:
(a) The roles and responsibilities of the internal role-players that are involved in the compliance process;
(b) The structural arrangements for the compliance function (information on the relevant structures and scope should be included); and
(c) The process to evaluate compliance - refer to Section 13 for a more comprehensive description of the compliance process.

(Section 13 focuses on (i) The determination of the universe of applicable, regulatory requirements for the business; (ii) The identification and evaluation of applicable compliance risks; (iii) The optimisation of control measures; and (iv) The monitoring of control measures, for example, by utilising a self assessment or control effectiveness evaluation process.)

(d) Statutory, regulatory and supervisory requirements

This section, which could be seen as an operational procedures manual, should focus on the statutory, regulatory and supervisory requirements that fall within the scope of the compliance function. It sets out the following for each requirement:

(i) A summary of the requirement, as well as its applicability to the business. A brief description of the impact that non-compliance to the requirement might have on the business should also be included. **It should be kept in mind that the original document remains the only authoritative source for the specific requirement and that the summary should only be seen as a synopsis.**

(ii) A Risk Management Plan containing a description of the prescribed internal procedures to ensure compliance. **Please note that the intention is only to include those sections/provisions of a specific requirement for which it is possible to implement an internal control measure to ensure compliance.**

(iii) A description of the review procedures to evaluate the extent of compliance (an examination checklist could be used for this purpose).

10.5 Conclusion

The manual should be comprehensive in the sense that it covers all matters relating to compliance for the business. It should, however, be user-friendly and easy to understand to ensure full implementation thereof by all staff members.
APPENDIX 6
EXAMPLE: Letter of Endorsement from the CEO

All Managers and Staff Members

Dear Sirs/Madams

RE: ESTABLISHMENT OF A COMPLIANCE FUNCTION

Ongoing changes to legislation, together with the introduction of new legislation, has placed a greater emphasis on the formal and structured monitoring of compliance to, regulatory requirements.

Although legislative changes place an administrative burden an opportunity is provided to commit more openly to a culture of compliance within the Group, its subsidiaries and divisions.

The XYZ Group Limited recognises its accountability and responsibilities to all stakeholders under the legal, regulatory and supervisory requirements applicable to its business. Therefore the Board of Directors has approved the establishment of an independent Compliance Function as part of its current Compliance Policy.

The Board is ultimately accountable to its stakeholders for overseeing compliance requirements. The responsibility to facilitate compliance throughout the Group has been delegated to the Group Compliance Officer who heads the Group Compliance Function. The Group Compliance officer is responsible for the effective implementation of the Group Compliance Policy.

However, it must be emphasised that the primary responsibility for complying with any regulatory requirement lies with each 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. Your staff members must understand that they are expected to comply both with the letter and with the spirit of these requirements.

The Board of Directors regards compliance as a matter of high priority. All staff must understand that failure to comply can result in exposing the Group to liabilities and/or risk of loss of authorisation to conduct business in the financial services industry.

There is a growing need for management to have professional support from the Group Compliance Function to identify potential problems and advise on practical solutions. Staff need to provide a constructive service to the business and must help to protect the reputation of the Group. This is not something that compliance officers can achieve on their own; there must be a determined team effort together with the management and staff of the business.

As part of this effort a compliance manual has been drafted. This manual documents how compliance should be conducted in a specific business unit by complying with the
relevant compliance policy and standards. In addition, it documents how all the applicable laws, regulations and supervisory requirements are being managed and controlled. Non-adherence to the standards documented in this manual can lead to disciplinary action and dismissal.

The importance of protecting the Group's reputation in all its operations cannot be overemphasised. An appeal is made to all staff to acquaint themselves with the contents of the compliance manual to enable them to meet the responsibilities in their work environment.

Yours faithfully

CHIEF EXECUTIVE OFFICER
11. ESTABLISHING POLICIES AND PROCEDURES

11.1 Introduction

Why should a business have policies and procedures in place?

Management is responsible for mitigating business risk and for ensuring compliance with regulatory requirements. How does management mitigate business risk and ensure compliance with regulatory requirements?

By creating a values-based compliance culture through the establishment of policies and procedures

11.2 Policies and Procedures

(a) Establishing policies and procedures

In order to be effective, policies and procedures should be established taking the following into account:

- Up to date in order to meet the continuously changing requirements;
- Relevant to staff members in their day to day activities;
- Detailed enough to address the operational requirements;
- Established within an appropriate governance framework, recognising that the board is ultimately responsible for the policies and procedures; and
- Supported by an appropriate level of "organisational buy-in" from both senior management and staff.

The compliance policy should illustrate the philosophy of the business on compliance. After reading a compliance policy, the reader should be able to identify and understand the business' perspective thereon and commitment thereto, as well the core values such as integrity, accountability and transparency. A compliance policy can vary in comprehensiveness depending on the specific need of the business. In some cases it may be fairly simple document for a small business whilst a more comprehensive document will be necessary for a large organisation with a complex structure.

The above is not exhaustive and is intended to serve as a high level indication of a number of important considerations.

(b) Compliance policy and procedures

Compliance policies and procedures will be established using available governance structures. They will serve as a cornerstone in the development of a compliance culture.

The formulation of a compliance policy provides a platform from which to communicate relevant compliance matters to staff members. A compliance

26©Compliance Institute of South Africa

Handbook for Members

March 2008
policy sets out what is expected from staff members, who are an integral part of an effective compliance system. This will, to an extent, determine the culture with regard to compliance.
(c) Core Elements of a compliance policy
The following serve as examples of elements that could be expected to form part of a compliance policy.

(i) Introduction
Information should be provided regarding ownership, approval, review, scope and implementation of the policy.

(ii) Compliance policy statement
The compliance policy statement should describe the business commitment and approach to comply with applicable legal and regulatory requirements. Although not always necessary, it could be helpful to base this statement on the vision, mission and core values of the business. An example of a compliance policy statement is as follows:

"The business 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. It is committed to comply with both the spirit and the letter of applicable requirements and to always act with due skill, care and diligence."

(iii) Philosophy
The philosophy provides general background information on compliance and usually covers aspects such as:

(1) The motivation for establishing the compliance functions;
(2) The history of the Compliance Function;
(3) The standards and norms that compliance is based on, for example, reference to standards and norms adopted by the Compliance Institute of South Africa (CISA); and
(4) Reference to other related philosophies in the business, e.g. the philosophy of the sales department, human resources, etc.

(iv) Framework
The framework should provide information regarding the following aspects:

(1) How compliance forms a part of the overall risk management framework; and
(2) A brief overview of a methodology to be followed.

(d) Responsibility for compliance policy
The setting of a compliance policy is the responsibility of the compliance officer. The compliance officer typically prepares this with input from stakeholders.

It is important that the policy is approved by executive management/Board of Directors. This will give it the status that is required for effective implementation thereof.

The Compliance Policy is a very important source of information
regarding compliance and should be widely distributed throughout the business. Care should also be taken to make this a very user-
friendly and practical document in order for all employees to be familiar with the content thereof.

(e) Compliance Procedures

Compliance procedures should be incorporated into the mainstream operating instructions that are in place. This process is often referred to as embedding compliance within business processes and documentation.

This is usually undertaken in the light of the regulatory analysis that is conducted with the assistance of the compliance officer.

For example, where a customer opens a new account with a financial institution, the requirements of the FIC Act should be taken into account in the account opening process as specified in the account opening procedures and documentation. This could include the following information gathering (as required by the FIC Act) on the account opening form in respect of a customer who is a natural person:

- Full names
- Date of birth
- Identity number
- Income tax registration number
- Residential address

(f) Compliance Standards

It may be beneficial to a business to develop high-level compliance standards that will provide the context within which the compliance procedures will be applied.

It is also noted that as compliance procedures can be lengthy, it may be difficult to achieve effective communication (especially at senior levels) without developing a high-level document that addresses the compliance challenges at a principle level.

Compliance standards could be structured under the following headings:

- Staff training
- Compliance manual
- Compliance monitoring
- Advisory services
- Compliance communication
- Regulators/Supervisors
- Customer complaints
- Objectivity and status
- Resources
- Access Control
- Group structure
- Acceptable business practices/Business ethics
- Compliance procedures
- Conflicts of interest

Each standard must be clearly specified. For example, the standard covering staff training could read as follows:

“Procedures must be established to ensure that all staff are aware of relevant regulatory requirements. These should address actions required of
staff in terms of regulatory requirements, as well as prohibited conduct. Staff must keep updated on any regulatory changes. This can be achieved through appropriate staff induction programmes, ongoing training, compliance briefings and compliance communications..."

11.3 Conclusion
The Compliance Policy is an important source of information regarding compliance and should be widely distributed throughout the business. Care should also be taken to make this a very user-friendly and practical document in order for all employees to be familiar with the content thereof.
12. COMPLIANCE RISK MANAGEMENT PROCESS

12.1 Introduction
We have seen that responsibility for complying with regulatory requirements rests with management. The compliance officer facilitates the implementation of a compliance system to manage regulatory risk.

Although the implementation of a compliance system will differ from business to business, the principles underlying compliance risk management will apply.

12.2 Phases in the Compliance Risk Management Process
The phases in the compliance risk management process are identified below.

<table>
<thead>
<tr>
<th>Phase 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Risk Identification</td>
</tr>
<tr>
<td>The compliance officer assists management in identifying the regulatory requirements that apply to the business.</td>
</tr>
<tr>
<td>All the regulatory requirements that have been identified together form the regulatory universe of the business.</td>
</tr>
<tr>
<td>The compliance officer assists management in analysing the regulatory requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Risk Assessment</td>
</tr>
<tr>
<td>The compliance officer assists management to prioritise the regulatory requirements by rating each according to their risk.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Risk Management</td>
</tr>
<tr>
<td>The compliance officer assists management to develop control measures that will ensure compliance and facilitate the implementation thereof.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Risk Monitoring</td>
</tr>
<tr>
<td>The compliance officer monitors the controls that have been implemented to determine the level of compliance and whether the controls are effective.</td>
</tr>
</tbody>
</table>
Compliance Risk Identification

Phase 1
Compliance Risk Identification

How does business comply with regulatory requirements if it does not know which regulatory requirements it must comply with?

Step 1
The first step in the compliance management process is to identify the regulatory requirements that must be complied with.

Definition
Remember that "regulatory requirements" is the term that is used to collectively describe the applicable "rules" set out in:
- Acts of Parliament
- Subordinate legislation
- Supervisory requirements

The applicable regulatory requirements are identified with reference to the South African regulatory universe, which is simply all of the regulatory requirements that are imposed in the country.

The compliance officer must obtain the relevant regulatory requirements. He/she must assist in identifying which of the requirements will impact on the business in a way that will require active compliance management. Once these have been identified, this will represent the regulatory universe.

Note: As it is not practical or achievable to actively concentrate on all of the applicable regulatory requirements, the job of the compliance officer is to rate the requirements according to the specific risk.

It is useful to identify the so called "top 20" requirements. An example of the aforementioned is set out below:
- Financial Intelligence Centre Act
- Banks Act
- Bills of Exchange Act
- Collective Investment Schemes Act
- Currency and Exchange Act
- Occupational Health and Safety Act
- Promotion of Equality and Prevention of Unfair Discrimination Act (PEPUDA)
- Securities Services Act
- Companies Act
- Home Loan and Mortgage Disclosure Act
- Usury Act
- Code of Banking Practice
- King II Code of Conduct for Corporate Governance
- Prevention and Combating of Corrupt Activities Act
- Long Term Insurance Act
Step 2
The next step in this phase of the compliance management process involves analysing the regulatory requirements.

Various approaches can be adopted in this regard. When analysing the regulatory requirements, it is important to note that different stakeholders will require different information. From a legal interpretation perspective, it is important to ensure that the technical detail is appropriately addressed. However, when communicating with management, the compliance officer should take care to describe the regulatory requirements in accessible terms, while still ensuring that the description represents an accurate interpretation.

In order to address the risk of misinterpreting the regulatory requirements, the full text thereof could be included in the risk management plan, together with a management analysis of the requirements.

Regulations 3 & 4 of the Financial Intelligence Centre Act will be used to illustrate how a risk management plan is used in the compliance risk management process.
(b) **Compliance Risk Assessment**

<table>
<thead>
<tr>
<th>Phase 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Risk Assessment</td>
</tr>
</tbody>
</table>

Once the identification and analysis of the regulatory requirements has been completed, they must be classified according to the risk thereof.

Why do we classify regulatory requirements according to risk? Although business must comply with all regulatory requirements, it is necessary to prioritise them to determine how often (the frequency) and how much (the extent) each regulatory requirement must be monitored.

Regulatory requirements can be categorised into:
- High Risk
- Medium Risk
- Low Risk

**How do you rate the risk of a regulatory requirement?**

In determining the risk rating of a regulatory requirement, there are two variables that must be assessed:
- Seriousness (the potential negative impact of non-compliance); and
- Probability (the likelihood of non-compliance occurring).

(i) **Seriousness**

"Seriousness" indicates the potentially negative impact that non-compliance with a regulatory requirement will have on the business as a whole. It is made up of the following elements:

- **Monetary impact:**
  This refers to the potential monetary loss, as a result of fines imposed or losses suffered due to non-compliance. The greater the amount of monetary loss, the greater the "seriousness" of the non-compliance.

- **Impact on image:**
  This refers to the extent to which non-compliance may impact negatively on stakeholders' perceptions. Stakeholders include regulators, investors, depositors, consumers, employees and government. The greater the potential negative impact on the image of the business, the greater the "seriousness" of the non-compliance.

(ii) **Probability**

"Probability" indicates the likelihood that non-compliance with a specific regulatory requirement might occur. This is determined by the effectiveness of the control measures that have been implemented.

The seriousness and probability considerations should be rated on a scale of high, medium and low to determine the compliance risk.
For those who prefer it in simple terms, to determine the compliance risk, consider it in the following terms:

- How much money might be lost?
- How bad will the business look?
- What are the chances that it will happen?

Those regulatory requirements that are rated as "high risk" require ongoing focus on monitoring, while those that are rated as "medium" or "low" risk require monitoring on a less frequent basis.

The risk rating should be included in the risk management plan. This will be illustrated in Phase 3 below on compliance risk management.
Now that the regulatory requirements have identified, analysed and prioritised, control measures must be designed and implemented to ensure that the regulatory requirements are complied with.

Control measures can be categorised under three headings:
- Policies and procedures;
- People; and
- Information technology systems.

Ideally, these control measures should be recorded in the risk management plan together with a target date for the implementation of the control measure.

In order to demonstrate the approach that could be adopted, regulations 3 & 4 of FICA are used to identify possible control measures that could be implemented to ensure compliance with the regulatory requirements. For the purposes of simplicity, the exercise is limited to regulations 3(1) & 4(1) (a) (i).

Risk management plans are a useful tool in implementing the compliance risk management process.

It is noted that a typical risk management plan includes the following fields:
- Section number and heading
- Regulatory requirement
- Analysis of the regulatory requirement
- Risk rating
- Control measures
- Monitoring plan
- Monitoring report

This could be undertaken using a multi-column table reflecting the above headings in each column, or alternatively through the use of a database that caters for each of these fields.
## APPENDIX 7
### EXAMPLE OF RISK MANAGEMENT PLAN

<table>
<thead>
<tr>
<th>Section No and heading</th>
<th>Regulatory requirement</th>
<th>Analysis of regulatory requirement</th>
<th>Risk rating</th>
<th>Control measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification and Verification FICA Regulations 3(1) &amp; 4(1)(a)(i)</td>
<td>3(1) An accountable institution must obtain from, or in respect of, a natural person who is a citizen of, or resident in, the Republic, that person's-(a) full names; (b) date of birth; (c) identity number; (d) income tax registration number, if such a number has been issued to that person, (e) residential address. 4(1) An accountable institution must verify the full names, date of birth and identity number of a natural person referred to in regulation 3 (1) (a), (b) or (c)...by comparing these particulars with (a) (i) an identification document of that person; or.....</td>
<td>In respect of South African citizens and residents, regulations 3 &amp; 4 compel an accountable institution to obtain and verify the following particulars in respect of a customer:  • Full names;  • Date of birth;  • Identity number;  • Residential address. income tax registration number (note - the above has been aimed at senior management. More detail would be required at an operational level)</td>
<td>High</td>
<td>All account opening forms must include fields where the following must be completed:  • Full names  • Date of birth  • Identity number  • Income tax registration number  • Residential address  A copy of the customer's identity document must be obtained to verify the customer's identity. Copies of documents, which verify the correctness of the above information, must be obtained and annotated &quot;original sighted.&quot; The copy must be date stamped and the name and designation of the staff member opening the account must be recorded thereon.</td>
</tr>
</tbody>
</table>
(d) Compliance Risk Monitoring

<table>
<thead>
<tr>
<th>Section No and heading</th>
<th>Monitoring plan</th>
</tr>
</thead>
</table>
| Identification and Verification FICA Regulations 3(1) & 4(1)(a)(i) | Select a sample of customer accounts which have been opened in the last 3 months and conduct the following monitoring procedures:  
- Review the account opening forms for and determine whether the following information has been captured:  
  o Full names  
  o Date of birth  
  o Identity number  
  o Income tax registration number  
  o Residential address  
- Scrutinise the copy of the customer's identity document and confirm that it is appropriately annotated, date stamped and the required details are recorded.  
- Agree the customer identification details as contained in the account opening forms to the document provided to verify the correctness thereof. |

Each of the phases of the compliance risk management process is described above.

The approach that is adopted in the rollout of the compliance process will depend on the particular circumstances of the business. It is noted that some adaptation may be required to meet the needs of each individual business.

12.3 Conclusion
The 4 phases of the compliance risk management process set out above represents an effective structure within which to implement an effective compliance system.

APPENDIX 8
ASSESSMENT SCALE
The assessment scale could be calibrated as set out below, namely, ratings between 1 and 10 allocated for Seriousness and Probability. The table provides a guideline which can be used to facilitate the ratings:

<table>
<thead>
<tr>
<th>Scale</th>
<th>Seriousness Key</th>
<th>Probability Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Insignificant impact</td>
<td>Low Risk (Fully effective)</td>
</tr>
<tr>
<td>2</td>
<td>Minor impact</td>
<td>Medium Risk (Partially effective)</td>
</tr>
<tr>
<td>3</td>
<td>Material impact</td>
<td>High Risk (Ineffective)</td>
</tr>
<tr>
<td>4</td>
<td>Material impact</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Material impact</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Material impact</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Disasterous impact</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Disasterous impact</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Disasterous impact</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Disasterous impact</td>
<td></td>
</tr>
</tbody>
</table>

![Regulatory risk profile: Statutory requirements for support functions]

[Graph showing the relationship between Seriousness and Probability with High, Medium, and Low Risk areas marked.]
13. COMPLIANCE TRAINING

Compliance training is a key factor in achieving effective compliance with regulatory requirements. Clearly staff members will not be able to effectively comply with regulatory requirements if they don't understand:

- The applicable regulatory requirements; and
- What must be done to comply with them.

13.1 Objectives of Compliance Training

(a) Introduction

Why is it important for a business to undertake compliance related training?
- Firstly, business needs to ensure that its staff understand their regulatory obligations to enable them to comply with the regulatory requirements that impact on their jobs;
- Secondly, to promote a culture of compliance;
- Thirdly, to ensure that staff understand the consequences of non-compliance; and
- Fourthly, because it is the law!

(b) To achieve effective compliance

Section 12 addressed the compliance risk management, as well as the need to design and implement control measures to ensure that regulatory requirements are complied with.

For these procedures to be effective, staff must be trained. Not only do they need to know and understand the procedures, they must know and understand the regulatory requirements that gave rise to the procedure. This will promote effective compliance as staff members will better appreciate the rationale behind the procedures.

For example: Staff should understand that all the procedures and documents that must be completed to properly identify a customer as required by FICA may help to identify criminals and ultimately stop crime!

In the final analysis, all staff members have a responsibility to conduct all business in compliance with applicable regulatory requirements. However, it is submitted that it is not appropriate to place the responsibility for compliance on any individual, unless that individual is not satisfactorily trained.

(c) To establish a compliance culture

"Involvement in the development and delivery of compliance training is also, however, the single most important contribution that the compliance function can make to the implementation and maintenance of the right culture." Newton, page 114.

One of the stated objectives of compliance training is to establish and maintain a compliance culture where all employees are not merely complying with the rules, but have adopted a value system whereby they embrace the objectives underlying regulation. To achieve this, they need to understand these objectives.
For instance, where staff members understand the rationale behind the reporting of suspicious transactions, they will report such transactions more effectively and frequently.

Employees cannot be expected to embrace the objectives underlying regulation when they do not understand those objectives. Through training, employees must be exposed to the objectives underlying regulation and understand how these are aligned to the objectives and values of the company.

(d) To ensure that employees understand consequences of non-compliance
Ensuring that employees understand the consequences of non-compliance will achieve efficient and effective compliance with regulatory requirements. It is necessary to consider not only the consequences to the business, but also to the individual employee.

Employees must understand the potential impact of non-compliance in terms of both monetary loss, by way of direct or indirect fines, and the possible impact on the reputation of the business.

Employees must also understand that non-compliance will impact upon their performance assessment that in turn may lead to disciplinary action and may also have legal consequences. For example, if an employee does not report a suspicious transaction, that employee is committing an offence and may be liable for prosecution!

Regulators have recognised the value that training adds in achieving effective compliance and are, through legislation and supervisory requirements, making it compulsory to train staff in respect of their compliance obligations e.g.

- Regulation 47(4) of the Banks Act provides that: “as a minimum the compliance officer of a bank shall ensure that compliance staff are trained on a continuous basis in order to ensure that they have adequate technical knowledge in order to understand the regulatory framework that applies to the bank, as well as the risks to which the bank is exposed.”
- Section 43 of the Financial Intelligence Centre Act provides that “an accountable institution must provide training to its employees to enable them to comply with the FIC Act and the internal rules applicable to them.”

The above is not exhaustive and is included for illustration purposes only. It demonstrates the increasing importance being placed on compliance training.

13.2 How Compliance Training could be undertaken

(a) Introduction
Now that the objectives of compliance training are understood, it is important to consider how compliance training could be undertaken.

Training should ideally be seen as an ongoing process is implemented in a structured/controlled way, as outlined in the following steps:
Step 1 — Identify training needs
Step 2 — Identify who requires training
Step 3 — Design/develop or source training material
Step 4 — Methods of roll-out
Step 5 — Assessment
Step 6 — Record-keeping

**Step 1: Identify training needs**
As in all other areas of compliance, training resources are not unlimited. Accordingly, a risk-based approach in prioritising training needs should be adopted. In phase II of the compliance process (described above) compliance risk assessment was looked at in order to determine which regulatory requirements should be prioritised. In determining the risk rating of a regulatory requirement, the following two elements were discussed:

- Seriousness (the potential negative impact of non-compliance);
- Probability (the likelihood of non-compliance occurring).

The greater the potential negative impact of non-compliance and the greater the likelihood of non-compliance occurring, the greater the risk. The high-risk regulatory requirements should be prioritised in terms of training needs.

For example, FAIS and FICA are considered high-risk and training on both of the relevant requirements of these Acts must be prioritised.

Training needs can also be identified by assessing information received from the likes of:

- Complaints received;
- Monitoring undertaken; and
- Instances of compliance breaches reported by management.

**Step 2: Identify who requires training**
The second step in developing a training programme is to determine who must be trained and what they must be trained on. It is not practical or economical to simply train all staff in respect of all the regulatory requirements.

New recruits should be given orientation training in basic compliance principles as well as on the compliance policy and values of the business. This is an early opportunity to instil a culture of compliance.

Most importantly, all employees must be trained in respect of those regulatory requirements that impact on their daily operations and in respect of which they are responsible for compliance. It is not fair to shift the burden of responsibility for compliance to an employee who has not been adequately trained.
Step 3:
Design or source training material
Now that the employees who must be trained have been identified, it is important to either design and develop or source the training material required.

While training material can be designed and developed in-house it remains extremely costly to produce. As compliance training is, to a large extent, considered to be non-competitive, a solution can be found in developing compliance-training material at an industry level. It is noted that the Inter-Bank Compliance Training Project has been successful in developing generic banking industry compliance training, specifically in respect of:
- Money laundering control;
- Financial advisory and intermediary services; and
- Occupational health and safety.

Step 4:
Methods of rollout
Before the various methods of rollout are considered, it is important to decide who should deliver the training material — the compliance function or management?

In most cases compliance training should be integrated into broader job-related training. This is an attractive approach, as the employee will tend to view the regulatory aspects as part of the job and not another layer of bureaucracy. Also, it always helps to have the person who is assessing an employee’s performance deliver the training as the message may seem clearer! Another advantage is that the line manager takes ownership of the training material and will have to master it before he can deliver it to others.

If it is not practical to integrate compliance training into the business related training of employees, for example, where the training needs relate to generic compliance obligations, it may be necessary for the compliance function to take charge of the design and delivery thereof.

Methods of rollout of training include:
- Facilitated training;
- Self-study; and/or
- CBT (computer based training).

Step 5:
Assessment
It is important to assess employees in respect of the compliance training undertaken. Not only is it important to know whether the training has been effective and whether actual compliance knowledge has been imparted, it also essential from a legal perspective.

As discussed earlier, certain legislation makes it compulsory to train employees. If the accountable institution does not provide the training as required in terms of Section 43 of FICA (see p54), the accountable institution will be held liable in the event of a breach resulting from
inadequate training.
Another example is the FAIS Act that requires that employees who provide advice must be ‘fit and proper’. If such an employee does not pass an assessment, the employer will be forced to suspend that employee from providing advice or otherwise it runs the risk of exposing itself to risk as a result of using staff that are not deemed competent.

**Step 6: Record-keeping**

Attendance registers must be kept of all employees who attend compliance training. Further, following an assessment, the results of the assessment should be kept.

These records are required as a means of proving who has received training and on what they were trained. It also provides evidence of the results of any assessment.

Compliance training is essential to the success of a compliance function.
14. COMPLIANCE MONITORING

14.1 What is Monitoring?
"A compliance function without a monitoring programme is like an elephant without a trunk: it smells nothing and has a vastly diminished profile" Newton

**Definition**
Monitoring in the compliance environment can be defined as:

'An examination of business activities to assist management and the board of directors to understand whether business is conducted in compliance with relevant regulatory requirements'.
APPENDIX 9

The Compliance Process

The text highlighted in red indicates where monitoring applies in the compliance process. The compliance process consists of the following four phases:

<table>
<thead>
<tr>
<th>Phase I Compliance Risk Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Identify all the applicable requirements that fall within the scope of the compliance risk. <em>(This should be done first for the business as a whole and, where applicable, thereafter for the individual Divisions/Subsidiaries)</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase II Compliance Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Categorise the identified requirements in terms of core, topical and pertinent or secondary.</td>
</tr>
<tr>
<td>3 Prioritise the identified requirements by rating each in terms of Probability and Seriousness. <em>(The provisions of each requirement should also be analysed and prioritised, if applicable, on the same basis)</em></td>
</tr>
<tr>
<td>4 Plot the requirements according to the ratings on a scatter diagram.</td>
</tr>
<tr>
<td>5 Classify requirements into high, medium and low risks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase III Compliance Risk Management (Control optimisation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Based on the requirements in the high risk area as priority, develop a Compliance Risk Management Plan for each requirement by identifying, <em>inter alia</em>, the following: (i) the provision(s) for each requirement that has to be complied with; (ii) the control measure that will ensure compliance; (iii) the responsible person for implementing the control measure and (iv) the target date for implementing the control measure (if applicable).</td>
</tr>
<tr>
<td>7 Include Compliance Risk Management Plan in the compliance manual.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase IV Compliance Risk Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Develop an effective review process to evaluate the implementation of the Compliance Risk Management Plans.</td>
</tr>
<tr>
<td>9 Report findings of the review process to the relevant role-players.</td>
</tr>
</tbody>
</table>
14.2 Why Monitor?

Brian Sharpe writing in his book, "Making Legal Compliance Work", makes the following comments:

"Effective monitoring aims to check that people are doing what they ought to be doing and that the system is operating satisfactorily. As monitoring is what frequently identifies problems, a failure to monitor adequately is likely to be regarded as showing a lack of real commitment."

The monitoring of compliance is an ongoing and potentially complex process that will vary from business to business.

One aspect that is likely to be present in all monitoring processes is an examination of all business activities to obtain reasonable assurance that these activities are conducted in compliance with relevant regulatory requirements. Applicable processes should therefore be in place to identify sensitive or high-risk areas of the business where non-compliance to these requirements is likely to occur and monitor these continuously at various levels.

Monitoring requirements may be incorporated into regulatory requirements. The following specifically makes reference to compliance monitoring:

**Banks Act - Regulation 47**

**Monitoring:**
- (g) Be responsible for establishing a compliance culture in the bank that contributes to the overall objective of prudent risk management by the bank;
- (h) Establish a line of communication to line management, in order to monitor continuously compliance with laws and regulations or supervisory requirements by the bank;
- (i) Require line management to monitor compliance with laws and regulations or supervisory requirements as part of their normal operational duties;
- (j) Require regulatory requirements to be incorporated into operational procedure manuals when appropriate; and
- (k) Make recommendations whenever necessary in order to ensure that there is compliance with laws and regulations or supervisory requirements.

**STRATE Rules**

7.4.3 The primary functions of the compliance officer shall be to review -
- 7.4.3.1 the daily monitoring, controlling and reconciling of the uncertificated securities accounts of the CSD participant.

**Policyholder Protection Rules**

15.5 Insurers and intermediaries shall, within 6 months from the date of coming into operation of these Rules, ensure that they provide -
- (a) For monitoring systems to measure compliance with these Rules.
Financial Advisory and Intermediary Services Act
17. (1) (a) Any authorised financial services provider with more than one key individual or one or more representatives must, subject to section 35(1) (c), appoint one or more compliance officers to monitor compliance with this Act by the provider and such representative or representatives, particularly in accordance with the procedures contemplated in subsection (3), and to take responsibility for liaison with the registrar.

Financial Advisory and Intermediary Services Act- Regulations
6. An authorised financial services provider shall ensure that any employee to be utilised as a compliance officer -

(c) Will, as regards the relevant business, have adequate resources available to ensure proper compliance monitoring, including as regards the activities of any representative, and have and be permitted direct access to, and demonstrable support from, the senior management of the business and in respect of any representative;

(f) Will be required to report immediately any instance of non-compliance to the provider, and be able to make recommendations to the provider as regards any aspect of the required compliance or the monitoring functions.

Financial Intelligence Centre Act
43 Training and monitoring of compliance
An accountable institution must-
(a) Provide training to its employees to enable them to comply with the provisions of this Act and the internal rules applicable to them;
(b) Appoint a person with the responsibility to ensure compliance by-
(i) The employees of the accountable institution with the provisions of this Act and the internal rules applicable to them; and
(ii) The accountable institution with its obligations under this Act.

14.3 Who Monitors?
The role players in the monitoring process are management, the compliance officer, regulators, board of directors, internal audit and external audit.

This section of the handbook deals with how the role players carry out their respective functions.

Compliance is more than just manuals and procedures and the extent to which this is correctly perceived depends totally on the effective interaction between the various role-players in the management compliance matters. Interaction between the role-players will only become effective once each of the role-players fully understand their individual roles (mandate).

It is noted that Compliance Risk Management Plans should ideally identify monitoring responsibilities relating to the applicable regulatory requirements, for example, the name of the responsible compliance officer or member of management is specified together with the time frames and details of the monitoring to be conducted.
One of the challenges facing business is to avoid duplication of effort by the different role players, whilst also ensuring that all the gaps are closed.

(a) Monitoring Role Players
The monitoring of compliance can take on various forms depending on:
- The level at which it is done; and
- The business conducting it, i.e. whether it is the entire organisation or a business unit.

This section focuses on the methodology for the monitoring of compliance by the compliance. The monitoring by the regulators and the management responsible for compliance is briefly mentioned.

(1) Compliance monitoring by Regulators
Monitoring of compliance by the regulators normally takes place at the highest level and includes all the entities subject to the specific regulator's supervision. The nature of the monitoring, as well as the process followed by the regulators, will depend on:
- The mandate of the regulator and the profile of the specific business;
- The proven consistency of the measures implemented to enhance a culture of compliance; and
- The relevant supervisory requirements.

(2) Compliance monitoring by Management
Compliance monitoring by management is another kind of monitoring that should take place as part of their normal operational duties. They are primarily accountable to the board of directors for compliance and the format and nature of the monitoring in this regard will depend on the specific situation, but ideally should be embedded into the systems of the specific business unit.

(3) Compliance monitoring by Compliance Officer
One of the compliance officer's responsibilities is compliance monitoring.

The compliance function may be centralised, decentralised or a combination of both. The structure that is put in place will clearly have an impact on the nature of the monitoring that is conducted.

The compliance officer should promote compliance awareness, which includes the training of business unit staff with regard to new legislation, amendments to legislation or adherence to existing requirements and act in a consulting role to management in the monitoring process.

The decentralised compliance officers are appointed by the individual business units and will be required to have specialist knowledge of the unit. Due to the close involvement in the business unit, the decentralised compliance officer's monitoring role should be focused on the day-to-day monitoring activities within the business unit, e.g. business unit dashboard and reviewing line management's monitoring activities.
In a centralised compliance structure, the compliance staff works with many business units and their role would tend to be more consultative in nature. As a centralised compliance function is more removed from the business unit, the independent monitoring responsibility should ideally rest with the centralised compliance function.

A combined structure consists of both a centralised and decentralised compliance staff that all report either directly or indirectly to the compliance officer. This structure is more appropriate to larger organisations.

One of the most comprehensive South African regulatory requirements relating to monitoring is currently Regulation 47 of the Banks Act No 94 of 1990. Although this Act is not applicable to all entities in the financial services industry, these provisions are based on sound risk management principles and can be applied to any business, irrespective of size. Monitoring of compliance in this context entails the following activities, as set out in Regulation 47:

- Establishing a compliance culture that contributes to the overall objective of prudent risk management;
- Establishing a communication line-to-line management in order to continuously monitor compliance;
- Requiring line management to monitor compliance as part of their operation duties;
- Facilitating the incorporation of regulatory requirements into operational procedures and appropriate manuals; and
- Recommending corrective steps to ensure compliance.

The above activities indicate the role that the compliance function should play in supporting management. In addition to this, compliance officers must also undertake compliance monitoring.

The level at which the compliance officer monitors compliance differs from situation to situation, but in general it could either be overview based or detail-orientated. In the case of an overview-based approach, the compliance officer will focus on exception reports and the follow-up of detailed non-compliance issues. This approach can be useful, as long as the reports are produced timeously and are accurate and comprehensive enough to cover all the business activities.

The choice of approach will be influenced by the maturity stage of the compliance function as illustrated in 18.4 below.

(4) Compliance monitoring By Board of Directors and Board Committees

The board is ultimately responsible for any financial loss or reduction in shareholder value, and therefore they have a duty to make the necessary enquiries to ensure that the requisite systems, practices and culture are in place to manage all compliance risks to which the
business is exposed. It is ultimately their responsibility to oversee that the business complies with applicable laws, regulations and supervisory requirements. These risk management/control responsibilities can be delegated to appointed individuals, committees and functions.
(5) **Compliance monitoring by Internal Audit**

The internal audit team should be involved in the monitoring process as monitoring can usually be combined with their normal activities. Whilst internal audit have the necessary skills to carry out the relevant checks, effective monitoring requires knowledge and training in the subject being monitored. It is therefore advisable, whenever internal audit is involved, that the compliance officer assists in the compilation of the monitoring programme. This is due to the highly specialised content of the regulatory requirements. In the final analysis, although the work of internal audit may be relied on by the compliance function, it is important that compliance reports independently to the board audit committee or management.

(6) **Compliance monitoring by External Audit**

The role of the external audit committee is to review the risk processes as part of their statutory audit and any other duties imposed on them by the Companies Act, Banks Act or any other legislation. It is their responsibility to assess the adequacy and effectiveness of internal controls and procedures with specific reference to laws, regulations and supervisory requirements.
MONITORING ROLE PLAYERS AND THE TYPES OF MONITORING THAT THEY UNDERTAKE

<table>
<thead>
<tr>
<th>Role Players</th>
<th>Routine</th>
<th>Independent</th>
<th>Objective</th>
<th>Oversight</th>
<th>Ad Hoc</th>
<th>Supervision</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOARD4</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIT/RISK4</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEO2</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MANAGEMENT2</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GROUP COMPLIANCE3</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BUSINESS UNIT COMPLIANCE3</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>INTERNAL AUDITS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>EXTERNAL AUDIT6</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>REGULATORS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

This table indicates the types of monitoring typically undertaken by the respective role players.

14.4 How and When to Monitor
This section covers how and when monitoring is undertaken. This is graphically illustrated in the diagram.
Although some of the control measures that will be identified in Phase III will comprise continuous monitoring activities by management, the formal compliance monitoring activity is the fourth phase of the compliance process.

It is typical that when a compliance function is initially introduced, monitoring will take some time to be implemented in an effective manner.

**Maturity**

The table below should be read in conjunction with the Compliance Process for Regulatory or Business Environment diagram on the previous page.

The development of a compliance function could be classified into 4 stages i.e.

- Stage 1 — Undeveloped
- Stage 2 — Developing
- Stage 3 — Developed
- Stage 4 — Fully Effective

*This table illustrates the possible relationship between the maturity level of the compliance function and the implementation of the different phases of the compliance process.*

<table>
<thead>
<tr>
<th>PHASE</th>
<th>UNDEVELOPED</th>
<th>DEVELOPING</th>
<th>DEVELOPED</th>
<th>FULLY EFFECTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>III</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>II</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Effective — No significant aspect of the compliance function requires development.
Developed — Largely effective, but there may be some aspects that require development.
Developing — There are considerations that require development in order to promote a fully effective compliance function.
Undeveloped - A large component of the compliance objectives are not being achieved.

Compliance monitoring activities can be broadly categorised as Ongoing/Routine monitoring and Independent monitoring. Ongoing Monitoring will be conducted during all stages of the development of the compliance function whereas independent Monitoring will usually only be undertaken in a 'Developed' and 'Fully Effective' compliance function.
14.4.1 Ongoing/Routine Monitoring

(a) Checklists
Checklists are a valuable part of monitoring and can either be utilised by line management or the compliance officer. If utilised by line management, checklists should be documented as a control measure. A checklist should be carefully compiled, as there is a danger that a checklist may be thought of as complete and representing all that needs to be done.

(b) Complaints Review
A business should have written procedures for the effective consideration and proper handling of customer complaints. Part of the compliance process would be the monitoring of customer complaints to establish possible areas of non-compliance. Complaints must be impartially considered by either the compliance officer or a member of line management of suitable seniority.

(c) Non-compliance Reporting/Tracking Procedure
A suggested non-compliance reporting/tracking procedure must be developed as part of a non-compliance database that is designed to allow business units to report incidents of non-compliance through to compliance. This type of database should be kept simple in terms of being able to access and use and the requirements/detail should be kept to a minimum. It is also important to take confidentiality into account when implementing this type of procedure, namely, the business units do not wish their issues of non-compliance to be broadcast to or accessed by other areas. This database should only be accessed by the compliance officer/s.

An example of the fields that could be contained in the database is as follows:

- Date of occurrence
- Division/business unit
- Description of the incident
- Seriousness
- Person/s involved
- Actions taken/to be taken
- Person responsible for action
- Date of resolution

A section blocked out from view to all the business units, which contains the compliance officer's comments, follow up and date of resolution.

(d) Dashboard
The dashboard is a tool or early warning device for ongoing monitoring that alerts the compliance officer to changes in the compliance environment that could lead to an increased probability of non-compliance occurring.
On a business unit level, the dashboard will typically be more detailed and focused on the business unit activities whereas a group dashboard
will tend to be more high-level; less detailed and focussed on the group compliance risk areas.

The success of a compliance dashboard depends on the accurate identification of the critical indicators. These indicators can be "leading" or "lagging."

Leading indicators monitor an increase in a certain action or activity that may indicate a higher potential of non-compliance occurring, for example, the level of new product development, business volumes, unusual levels of sales, decrease in training, etc.

Lagging indicators monitor actual breaches, for example, fines, complaints, prosecutions, etc.

Ideally, the dashboard should be automated and linked into the business units' management information system.

(e) Issues Log
The compliance function should compile a list of all issues identified during all types of monitoring activities. They should ensure that management implements corrective measures and that the implementation is followed up.

(f) Walking Around
Line management should be actively involved with staff at all levels in order to be able to quickly identify issues of non-compliance.

(g) Physical Checks
Line management needs to physically check that the procedures and other controls are being carried out.

(h) Management Information Systems/Exception Reports
Information/Exception reports can be extracted from operational systems to indicate possible risk areas based on any number of preset criteria.

(i) Mystery Shopping
Compliance officers can identify exceptions through mystery shopping. For example, this may entail the compliance officer or appointed person actually opening an account at a bank branch to identify whether staff members correctly follow the designated procedures in practice.

14.5 Independent Monitoring
Independent monitoring consists of control adequacy reviews, control consistency reviews and substantive reviews and is the most extensive monitoring activity.

This compliance monitoring process requires the compliance officer to perform a series of procedures and activities:

The main stages of this monitoring process include:
• An updating of the business background information that is to be reviewed;
• Review planning;
• Compliance (control adequacy and control consistency) and substantive procedures; and
• Reporting the results of the review.

The methods used to obtain information to produce the aforementioned output take the form of questionnaires, one-on-one discussion, workshops and stand-alone work, for example, walkthrough reviews and analytical reviews.

(a) Scope and Limitations
The scope of any review must be defined and all limitations must be documented.

(b) Resources and Scheduling
A compliance review might require a multi-disciplinary team, for example, a tax or computer expert or audit staff in addition to the usual compliance staff. The review has to be conducted in a systematic and orderly manner to ensure the smooth running of the assignment within a reasonable time frame. Factors such as costs and minimum disruption have to be seriously considered.

All team members and any specialists that may be engaged on the compliance review must be identified and documented during this phase to take the aforementioned into account.

(c) Independent Monitoring Techniques
These involve the following:
• Adequacy and Consistency Reviews; and
• Substantive Reviews.

(d) Independent Monitoring Approach
The review of the controls begins at this stage. The compliance officer needs to test whether the control measures that were implemented to ensure compliance are adequate and consistent. These control measures are normally recorded in the risk management plan.

The approach involves firstly reviewing whether a control is adequate.

(1) Adequacy Review
Adequacy review involves the review of the existence of a control and whether it reduces the risk to a level acceptable to management.

The compliance officer can use the following methods to obtain evidence on adequacy:
• Interviews or enquiry — oral evidence.
• Observation — watching a procedure, for example, observing whether an employee, who has transgressed a rule and is to be dismissed, is asked the appropriate questions at the inquiry to ensure that the dismissal meets with the procedural requirements.
• Reperformance — reperforming what should have done, e.g. reconciliation, or recalculating the client's calculation of Estate Duty to ensure that it complies with the requirements of the Estate Duty Act.
• Vouching — comparing information in a book of record to a source document, for example, the information in the Register of Directors Interest in Contracts could be vouched to the director's written declaration, which is circulated at or before the directors' meeting.
- **Verification** agreeing information to other sources, for example, the DIO20, which is a form that must be submitted to the Registrar of Banks whenever a new director is appointed.
- **Walkthrough review** following a procedure through from its inception to its conclusion.

If we agree the minutes of the annual general meeting with the copy of the return submitted to the Registrar of Banks (book of record to a source document), this would be vouching and if we agree the minutes and return to the confirmation letter received from the Registrar of Banks, this would be a verification procedure (agreeing information to other sources of information such as from a third party).

The test for existence involves selecting only one item from a population. The adequacy test must be documented in a working paper, which serves as evidence of the work done and any pertinent information gathered and should state whether the control is adequate or inadequate.

If a control is adequate, then its consistency must be reviewed.

---

**The sequence of the reviews are illustrated schematically as follows:**

![Diagram]

---

63©Compliance Institute of South Africa

Handbook for Members
(2) Consistency Review

A consistency review involves reviewing whether the adequate control has been applied consistently throughout the period under review. It may not be practical or cost effective to test whether the control has been applied to every item in a population throughout the period under review. A sample that represents the population would therefore have to be selected based on the various sampling techniques indicated below - refer Paragraph 4.2.5 (e).

The techniques referred to In Adequacy Review can also be used in conducting consistency reviews.

Reperformance, vouching and verification are relatively reliable forms of evidence, as these are supported by documentation.

The steps in a consistency review are as follows:

(i) Determine Scope
(ii) Sample Selection
(iii) Testing of Items
(iv) Reporting of Findings

The abovementioned steps are illustrated in the following example:

(i) Determine Scope

For the purpose of this example, it would be assumed that the scope of the review covers a reporting period, for example, the previous financial year. (Also refer to Materiality discussed in paragraph 4.2.5 (d) below).

(ii) Sample Selection

If during a financial period, a 100 transactions have taken place, these 100 transactions, numbered 150 to 250, make up the population. A sample must then be selected (of say 30 items), from this population of 100 items. These 30 items will be reviewed.

The items could be randomly selected by using a computer programme that prints out the resolution numbers that have to be tested. (Please also refer to paragraph 4.2.5 (e) below regarding Sampling for more information).

(iii) Testing of Items

The items are tested and the results indicate that one item is not in line with the controls. A further sample could be selected for every item that is not in line with the control. The reason for the increase in the sample size is that the compliance officer requires further evidence that the sample is representative of the population, namely, in view of the exception found. If further sampling reveals that all items are in order, the conclusion that could be reached is that the controls are effective. If any of the items in the extended sample group are not in line, the conclusion is that the controls are ineffective.

The work done, which includes the provision/requirement, control, method of sample selection, results of the test, the computer generated
samples and the conclusion reached must all be recorded in the working papers.

(iv) Reporting of findings
If required, the compliance officer will bring a finding to the attention of management. Ideally, this should include recommendations for any challenges identified.

(3) Substantive Review
Substantive review is performed to gather evidence to support the compliance review report, namely, to obtain evidence relating to compliance with regulatory requirements.

Substantive procedures include computation, inspection, reperformance, enquiry and confirmation, analytical procedures and observation.

In the external audit environment, substantive review is used to verify the existence, ownership and valuation of assets and liabilities.

From a compliance perspective, compliance officers will seek to substantiate whether business activities are conducted in accordance with applicable regulatory requirements. This will involve the use of various tools or techniques, for example:
- Computation - computation involves performing checks for accuracy on calculations furnished, or when a compliance officer performs independent calculations and compares them with the calculations already done.
- Inspection - inspection provides audit evidence, which is mainly documentary. Documentary evidence can be created by the business or by third parties. Documentary evidence that is obtained from third parties provides greater reliability to the compliance officer.
- Reperformance - reperformance involves the compliance officer repeating a procedure originally performed by the business either completely or in parts.
- Enquiry and confirmation - the compliance officer obtains information from within or outside the business either orally or in writing.
- Analytical procedures - analytical procedures are the analysis of information to identify trends, fluctuations and relationships that are inconsistent with other relevant information or deviate from a standard amount. An example of a substantive review is the use of graphs to monitor fluctuations between liquid assets and reserve balances. A steep fluctuation would serve as a detection control that would alert management to take the necessary action to correct the situation. The Banking Council also requires a trend analysis on personal account trading which must be reported to the board of directors. This is done by applying analytical review procedures.
- Observation - the compliance officer observes a process or procedure that is being performed. This technique is usually carried out where the performance of a control procedure does not leave an audit trail.

(e) Materiality
It is not always practical and cost effective to test all items or transactions. The compliance officer therefore has to focus the review on the prioritised risks. Accordingly, materiality must be addressed in compliance monitoring.
Materiality, which is very subjective, could be quantitative (amount) or qualitative (judged by a factor other than an amount).

In determining whether an item is material, the following factors can be taken into account:

- The regulatory sanction;
- Fines and penalties;
- Operational losses; and
- Reputation.

Probability and seriousness ratings could also be applied to determine the materiality levels, where only items above a certain probability and seriousness level will be reviewed.

The manner in which materiality is determined depends on the type of Act or provision that is being reviewed.

(f) Sampling

Why is sampling used?
The compliance officer has to obtain sufficient and reliable evidence to express a valid and credible opinion. It is virtually impossible to review every transaction, due to the size and complexity of larger organisations and the cost factor involved in a 100% review. The compliance officer therefore has to select a sample of items within a population, which is then tested and the findings are evaluated in order to draw a conclusion.

Sampling Terminology:
(i) Population: This is the entire set of data or items from which a sample is selected and on which the compliance officer will draw a conclusion. For example, a population could be all Trust Departments, or all bank reconciliation's at a branch for the 2000 financial year-end.
(ii) Sampling Risk: Is the risk that the compliance officer's conclusion, which is based on the sample selected, may be different from the conclusion that he would have reached if he tested the entire population.
(iii) Sampling Units: These are the items that make up the population
(iv) Review Sampling: This involves the application of review procedures to less than 100% of the items in a population.
(v) Tolerable Error: This is the maximum number of errors in a population that the compliance officer is willing to accept and still conclude that the result from the sample has achieved the stipulated objective.
(vi) Materiality: The level of materiality set by the compliance officer and management will determine the extent of the review done.

Sampling Methods
The compliance officer has different sampling methods that can be used. The method of sampling that is chosen depends on the nature of the population and the objective of the test. This is illustrated in the discussions on the various methods below. Compliance officers may outsource the selection of sample to internal audit, for example.
The compliance officer can use a statistical or non-statistical approach to select his/her review sample.
Statistical Sampling:

Statistical sampling has the following characteristics:

- Can be randomly selected (use of computer programme) where every item in the population has an equal chance of selection; and
- Can be systematically selected (use of a computer programme) where the first item is randomly selected and then say every 10th item is selected.

Statistical sampling methods are:

- **Monetary Unit Sampling** - where every rand item in a population has an equal chance of being selected. This technique is usually used in Substantive Review. High rand value items are selected first until the cut-off rand value is reached. For example, if a cut-off or materiality level is R80. There are 22 items in a population totalling R100 as follows:
  1 = R 50; 2 = R20; 3 = R10; 4 = R5; 5 = R2; 6 = R2; 7 to 12 = R1 each and items 13 to 22 = 50c each. Monetary unit sampling will select items 1, 2 and 3 which = R80. Therefore the review sample will consist of only three sampling items, which comprise 80% of the population.

  The Banks Act requires sector classification of advances from banks. Monetary unit sampling can be applied to test whether items are classified correctly. Selecting the largest items under each sector classification speeds up the process.

- **Sampling for attributes** - calls for yes or no, right or wrong answers is usually used to estimate the number of errors or some other characteristic in a population. This sampling is concerned with the number of items and not the value of the items. For example, the number of forensic reports that are submitted after the 7-day deadline period. The more variable the items in a population, the larger the sample size needed - this is determined with reference to statistical tables.

  For example, if all the characteristics are either 'yes' or 'no', then there is no great variability. A formula consisting of two parts is used in calculating the sample.

- **Discovery Sampling** - This sampling method is used when a compliance officer is examining populations where the existence of gross error is suspected. These populations may include, for example, non-existent collaterals for a loan. Here statistical tables are used to establish the population but the number of errors in the sample size has to be stipulated.

- **Non-Statistical Sampling** - Non-statistical sampling methods include haphazard and judgemental sampling techniques:
  - **Haphazard Sampling** - this technique attempts to select randomly by avoiding bias and predictability. The compliance officer would manually select any item or say a sample of 30 items from a population of 100. There would be no specific logic to the items selected.
  - **Judgemental Sampling** - this technique is based on the compliance officer's judgement and is subjective. For example a compliance officer may identify a period of high risk, i.e. the six-month period when the compliance staff member responsible for the submissions of returns to the Reserve Bank was on secondment and other less experienced staff members had to perform this...
function. The compliance officer would select their sample of items from this period.

Sampling methods and samples must be documented in working papers.

In principle, if the sample reveals errors or concerns, the sample size should be expanded, taking into account the circumstances and nature of the findings. For example, it may be appropriate to expand the sample size by one third for each error found, however, this will depend on circumstances and is not a general rule.

14.6 Working papers
The compliance officer must keep working papers to provide evidence that the compliance review was conducted with the required degree of care and skill and to support the opinion given. The end product of the review process is the compliance review report, which is handed to senior management, the executive committee, the audit and compliance committee, as appropriate. The compliance officer must arrange the findings in the working papers and reference such findings in a logical way that it easily feeds into the compliance report.

Working papers should conform to three basic rules:
- Properly organised;
- Completeness; and
- Clarity and conciseness.

Working papers should also take the following matters into account:
- Documentation — the manner in which the information is arranged should be consistent — preformatted working papers meet this requirement.
- Objective of the test, scope and regulatory requirements, section/subsection and provision— must be clearly stated on the working papers.
- Work done/comments — the manner in which the sample was drawn and the actual work done etc.
- Conclusion — the conclusion reached by the compliance officer on the work done.
- Results should consist of the following:
  - Findings to be communicated to management (this is when non-compliance has been identified).
  - Effect of this non-compliance must be explained.
  - Recommendation/s — the control that must be implemented to ensure compliance to the relevant requirement/s.
  - Management comments - consists of the response to the above which must also be documented.
- Indexing and cross-referencing;
- Supervisory review- to be completed in the review notes section of the working paper; and
- Ownership — name, signature and date on every working paper.
APPENDIX 11

EXAMPLE OF WORKING PAPERS
An example of a working paper follows:

<table>
<thead>
<tr>
<th>Business Name</th>
<th>WORKING PAPER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>Signature and Name:</td>
<td></td>
</tr>
<tr>
<td>Compliance officer</td>
<td></td>
</tr>
<tr>
<td>Compliance Manager</td>
<td></td>
</tr>
</tbody>
</table>

Regulatory Requirement:
Section/ Subsection:
Provision:
Objective:
Scope:
Test:

Work Done:

Results:

Conclusion:
14.7 Evaluating, Concluding and Reporting

(a) **Introduction**

During this final phase of the compliance review process, the evidence that was gathered and committed to working papers must be evaluated to determine whether the evidence is sufficient and appropriate. The reported conclusion must be based on the evaluation of the person responsible (usually the manager) for the review.

There should be a flagging and follow-up system to ensure that the matter/problem is resolved or dealt with properly. This system will be the responsibility of line management. The compliance officer will facilitate and advise on these systems.

(b) **Objectives of a Compliance Report**

The compliance report is the end result of the compliance review process. It is therefore important that the objectives of this final document are clearly established.

Some objectives of this document are as follows:

(I) **To highlight control issues to management**

The compliance review report can play a major role in warning management of the potential danger in a situation where the control implications have not been properly addressed. This would be particularly relevant where new legislative issues apply to the business relating to the management's business objectives. For example, the obligations of the business in terms of the Skills Levy Act, could adversely affect the business's objective of maximising profit. However, with good controls in place, management may be able to recover moneys from the Fund.

The report should address the positive and the adverse findings of the compliance review. The reporting of positive findings provides management with the assurance that controls are sound and are in place. The report of adverse findings serves as a preventative tool as it alerts management on what action needs to be taken. The adverse report on controls may be as a result of controls falling into misuse after management had implemented a plan of action previously. In cases such as these, the review report must support management so that the issue reported is not construed as criticism.

(ii) **To Bring Problems To Management's Attention**

The highlighting of problems would be an expectation of the compliance review and must be brought out in the report. It is imperative that the compliance officer keeps properly documented working papers of the work done, the results and the conclusions reached and that the evidence is sufficient to support the findings on certain reported matters.

When a problem is reported, the deficiency should be noted as well as the underlying causes of the deficiency, for example, that a supervisor is overriding the control, as well as the effect of the deficiency. It cannot be overemphasised that the information obtained during the review must
be clearly documented, referenced and well thought out in order to correctly report the effect of a breach or non-compliance to management.

A few examples of issues that could feature in the effect of the deficiency aspect of the report are cost-benefit analysis, further illustrations on how things could get worse if the control is not adhered to and setting out a percentage or a rand value of the breach and its effect in terms of fines and penalties.

(iii) Recommending Change
This is a crucial aspect of the report which must be thought about creatively by the compliance officer in order to find solutions to any problems that arise. The recommendation/s must clearly state what is recommended and reasons for the recommendation/s.

Expressing a deficiency, its underlying causes and its effect, will give the compliance officer a logical foundation that will assist in making recommendation/s.

For example, if a non-adherence to a control is identified and the underlying cause of this deficiency is an overriding of the control by a supervisor. The effect of the deficiency is a fine of Rm for non-compliance with a regulation. The recommendations made by the compliance officer may include that the supervisor is given a warning to adhere to the control and the manager oversees that the supervisor adheres to the control.

If there is more than one option available to address the non-adherence to the control, the alternatives should be set out in the recommendations. However, the compliance officer must beware of providing an overload of advice in these situations.

The recommendation may attempt to get management to do things differently or it may attempt to remove underlying problems.

If possible, the cost of the recommendation or other resources should be indicated. The recommendation would be particularly convincing if the cost-benefit advantage of the recommendation is demonstrated. The cost of a poor existing control could be used as a comparison to the one recommended.

Where a control cannot be implemented immediately, a standard may be established that may be aimed at over a period of time.

The recommendations made must take the business environment into account and must also be practically workable.

The following terminology may be applied, depending on the seriousness of the recommendations:
"We recommend that the....."
A.

"We strongly recommend that the...."
"It is advisable for management to implement the....."
"It is essential that management puts the ......"

"Management needs to urgently address the issue of....."
"Management should consider these possibilities..."

Recommendations should also be presented in the report in order priority so that the matters of highest impact are read first.

(iv) Content of Report
The compliance report could contain the following:

1. **Executive Summary**
   All reports should start with an executive summary. The objective of this summary is to highlight to senior management, in a nutshell, what was identified, what was done and what action still needs to be taken.

2. **Formal Acknowledgement**
   For co-operation and assistance during review.

3. **Responsibility for Compliance**
   It must be expressly noted that responsibility for compliance rests with management and not the compliance officer.

4. **Objectives, Terms of Reference and Scope**
   The objectives, terms of reference and scope must be clearly stated in the report. These paragraphs must be cross-referenced to working papers for easy reference in future. The findings and the effect of the findings must be clearly stated in the report.

5. **Issues, Recommendations and Action**
   There should be a clear link between the terms of reference, issues and recommendations. The required action steps should be stated in descending order of importance with the highest priority being stated first. These paragraphs must be cross-referenced to the working papers that support them for speedy reference. The management comments to the recommendations should also be stated in the report.

6. **Conclusion**
   This stage follows the reporting stage when the entire compliance review is tied up and the matter may be put to rest until the next review.
   
   The quality review should also be done at the conclusion stage of the compliance review.

   Completed checklists and signoff sheets may be included in the file to confirm that the matter is concluded.

(v) **Quality Assurance**

1. **Introduction**
   Standards must be established and guidance must be provided on the quality control policies and procedures of a compliance function.

   Quality control policies and procedures should be implemented at two levels, the compliance division as a whole and to the compliance reviewers on an individual assignment.

72©Compliance Institute of South Africa

Handbook for Members

March

2008
SECTION 14

(2) The Compliance Division
The compliance division should adopt the following control procedures:

- Professional Requirements - independence, integrity, objectivity, confidentiality and professional behaviour.
**Skills and Competence** - the division should be staffed by personnel that have attained the required degree of professional competence to carry out their tasks with due professional care. Furthermore, staff should keep up with regulatory changes and have knowledge of the business and regulatory requirements.

**Assignment** — the compliance assignment is to be assigned to personnel that have the required degree of technical competence, training and proficiency for the specific requirement. Information must be properly documented and reported and followed up on where necessary.

**Delegation** — there must be sufficient direction, supervision and review of work at all levels to provide reasonable assurance that the work performed meets the appropriate standards of quality.

**Consultation** — there should be consultation within or outside the division and with specialists where necessary.

**Monitoring** — the adequacy and consistency of the quality control policies and procedures is to be monitored.

### Individual Assignments

The compliance officer should implement the quality control procedures that are the policies and procedures of the compliance division, to the individual reviews as well. The following could be adopted:

**Direction** — The compliance team to whom work is delegated need appropriate direction on their responsibilities and the objectives of the procedures to be performed, nature of the business, budget constraints etc.

**Supervision** — This involves monitoring the progress of the review, assisting the junior compliance officers with queries and issues requiring professional judgment.

**Review** — The work performed by each assistant needs to be reviewed by personnel of at least equal competence to consider whether or not:

> The work has been performed in accordance with the programme.
> The work performed and the results obtained have been adequately documented.
> Significant matters have been resolved.
> Objectives of the review procedures have been achieved.
> Conclusions expressed are consistent with the results of the work performed and support the compliance opinion.

An independent quality assurance reviewer, not otherwise involved in the review, should perform the review procedure before the report is issued.
### Example 1
Assuming that the scope of this review is for the period 1 March 2000 to 28 February 2001. The secretarial department controls 100 companies that are subsidiaries, associates or joint ventures of the holding company.

<table>
<thead>
<tr>
<th>PROVISION</th>
<th>CONTROL</th>
<th>TEST</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 179 of the Companies' Act: Annual General Meetings</strong></td>
<td>The risks with regard to the provision is the Following:</td>
<td>Adequacy —</td>
</tr>
<tr>
<td></td>
<td>1. That a meeting may not be held for some or other reason or that the</td>
<td>1. Enquire (enquire) from management as to whether a schedule exists</td>
</tr>
<tr>
<td></td>
<td>meeting may be held but not within the period as prescribed by the act.</td>
<td>in respect of all the companies and haphazardly inspect (inspect)</td>
</tr>
<tr>
<td></td>
<td>2. The following control may exist, if it does not exist, then the</td>
<td>the schedule for any one company for the current financial year's</td>
</tr>
<tr>
<td></td>
<td>control may be recommended as a new control to be implemented.</td>
<td>annual general meeting date</td>
</tr>
<tr>
<td></td>
<td>The control is therefore the following:</td>
<td>to ensure that the date for the annual general meeting is within not</td>
</tr>
<tr>
<td></td>
<td>(i) A schedule, which clearly sets out dates when activities are to be</td>
<td>more than nine months after the financial year-end and within not</td>
</tr>
<tr>
<td></td>
<td>carried out, exists. Once an activity has been carried out the planning</td>
<td>more than fifteen months between meetings.</td>
</tr>
<tr>
<td></td>
<td>date for the next activity or for the next year is immediately entered</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ii) The maintenance of this schedule is the responsibility of a clerk.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iii) A manager inspects the schedule on a monthly basis and signs the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>schedule as evidence that the dates are correct.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the control exists and the test has been successful then the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>compliance officer may report that the control is adequate and move</td>
<td></td>
</tr>
<tr>
<td></td>
<td>onto consistency REVIEW.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the control was not implemented but the meeting did take place</td>
<td></td>
</tr>
<tr>
<td></td>
<td>within the correct time then the compliance officer must also</td>
<td></td>
</tr>
<tr>
<td></td>
<td>enquire as to whether there may be a compensating control in place</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to ensure that the meeting took place within the prescribed time. The</td>
<td></td>
</tr>
<tr>
<td></td>
<td>compliance officer may then test the consistency of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>compensating control.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
If the compliance officer finds the compensating control to be effective, he may report that the control is effective.
If the control is not implemented and there is no compensating control, the compliance officer may report that the original control will be adequate when it is implemented.

Consistency
a) Randomly select 25 companies and inspect the March 2000 to 28 February 2001; and
b) Inspect the dates per the schedule to ensure that the annual general meetings per the schedules were all held within the prescribed periods; and
c) Where the meetings have already taken place within the prescribed periods whether the schedule is updated for the following year.

Assume that the controls are found to be ineffective, and then the compliance officer has to determine whether he needs to do substantive REVIEW.

The compliance officer then needs to establish whether the non-compliance with this provision will result in monetary loss to the companies or the holding company and quantify the monetary loss.
Assuming that there will be a significant monetary loss if the provision is not followed then the following substantive procedure may
<table>
<thead>
<tr>
<th>PROVISION</th>
<th>CONTROL</th>
<th>TEST</th>
</tr>
</thead>
<tbody>
<tr>
<td>be followed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) - Enquire (enquiry) from the company secretary whether the Annual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Meeting has been held; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) - Inspect (inspects a document) the attendance register of the directors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>and members to ensure that they signed as being present at that meeting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) - Inspect the minutes to determine whether the meetings were held on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the correct dates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Act also prescribes that the following matters must be dealt with at</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the Annual General Meeting:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Acceptance of the Annual Financial Statements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Appointment and Remuneration of Directors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Appointment of Auditors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1) A preformatted agenda, which sets out the prescribed matters to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>be discussed at the meeting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) A checklist which the company secretary ticks at the meeting to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ensure that all prescribed matters are discussed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(3) The company secretary documents minutes, which are preformatted with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the issues to be discussed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Substantive REVIEW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1) Inspect a sample or 30 minutes of meetings held to ensure that all</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prescribed matters have been dealt with as prescribed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX 13

Example 2

Banks are required to submit returns to the Reserve Bank. These returns are for the Bank to confirm that certain requirements of the Bank’s Act are complied with. The compliance officer conducts adequacy, consistency or substantive review on the controls or information in place in order to confirm to the Reserve Bank that it complies with these regulatory requirements.

<table>
<thead>
<tr>
<th>PROVISION</th>
<th>CONTROL</th>
<th>TEST</th>
</tr>
</thead>
<tbody>
<tr>
<td>The DI 820 return that the Bank Compliance Function has to complete is that the Bank is complying with the average minimum amount of liquid assets, as provided for in section 72 of the Act?</td>
<td>A manager in charge in the Treasury department reviews the liquid asset records as a percentage as well as in Rand value on a daily basis and signs the liquid asset register to confirm that the minimum amount of liquid assets held by the Bank at the close of business on any day during the holding period did not decrease to an amount less than an amount equal to 75% of the average daily amount of liquid assets required to be held? The manager in the Risk Management department monitors the balance on a weekly basis and signs the register to confirm this amount.</td>
<td>Adequacy Review: Select any one-day and inspect the register for evidence of the Treasury Department manager’s signature confirming that the daily balance complies with the Act. Select any week and inspect the register to confirm that the daily balance complies with the Act. Consistency Review: Randomly select 10 days of a month in the current financial year and inspect the register for evidence of the Treasury Department manager’s signature confirming that the daily balance complies with the requirements of the Act. Randomly select 10 weeks of the current financial year and inspect the register for evidence of the Treasury Department manager’s signature confirming that the daily balance complies with the requirements of the Act. Substantive Review: Calculate the average amount of the liquid assets during a holding period. Calculate 75% of the average amount of the</td>
</tr>
</tbody>
</table>
### TEST

liquid assets. Randomly select a sample of 10 days and inspect the minimum amount of the liquid assets of the bank on those days. Compare the minimum amount with your calculations per 2 above to ensure that the minimum amount did not decrease to less than 75% of the average daily balance.

### Conclusion

Compliance monitoring is one of the cornerstones of the compliance function. The application thereof will depend on the monitoring objectives and on the circumstances.
15. COMPLIANCE AWARENESS

15.1 Introduction
The objective of this Section is to establish a compliance culture and to facilitate a program to enhance this compliance culture.

15.2 Background
The program will be divided into two important subsections, i.e., the general awareness program for the employees and a formalised intensive training program of Compliance Officers or any employee whose job contains specific compliance tasks or responsibilities.

15.3 General Awareness Program ("GAP")
The general awareness program is the ultimate responsibility of line management. The Compliance Officer's responsibility is to advise on the program and to facilitate the program.
The two essential elements of the GAP are EDUCATION and REGULAR COMMUNICATION.

15.3.1 Education
Education ensures that employees understand the relevant topic. Education needs to be carried out by a number of means and repeated at intervals. The methods that could be used are:
i) Circulars
ii) Manuals
iii) Booklets
iv) Presentations
v) Briefings

A manual is an educational document and it serves as a practical day-to-day operating document.

The presentation and briefings should be compulsory for all employees and management. Records should be kept of the employees attending these presentations and briefings.

A company must have adequate arrangements in place to ensure that employees and management are educated on a continuing basis, therefore education on new regulations and laws are important.

Compliance monitoring will indicate all the areas that the employees do not comply with. These areas would need to be emphasised and the education program would be adjusted accordingly to accommodate these areas.

The content of courses presented to employees, as part of the GAP should be in practical and simple so that it is understandable at all applicable staff levels.
The purpose of GAP is to ensure that all employees and management do their respective tasks within fit and proper standards and that they maintain high standards of integrity and fair dealing. New employees should be educated and made aware of the company’s commitment to compliance with the law and regulations and informed that a similar commitment will be required by them.

15.3.2 Communication
Communication reinforces the compliance system’s importance to all employees and management and ensures that they remember the items with which they have to comply. Communication should be brief and easily absorbed and should be designed just to jog the memory. The methods for communication should include:

(a) Oral presentation;
(b) Short articles or reminders in internal journals;
(c) Messages on electronic mail system; and
(d) Even occasional posters.
Communication overlaps with education and should be two-way. Communication from the workplace back to the Compliance Officer should be encouraged because it will:

(i) Express ideas;
(ii) Facilitate the resolution of problems;
(iii) Note difficulties in a system that needs improving; and
(iv) Assist employees to feel comfortable about seeking help.

15.4 Formalised intensive training program
This program ensures that those who have to carry out compliance tasks and responsibilities understand how the job fits into the wider context and they know how to perform the necessary function. Compliance training is needed for those whose jobs contain specific compliance tasks or responsibilities. Compliance staff should receive specific training in types of monitoring techniques used by internal audit. They may also need training in matters such as scheduling compliance activities, effective communications, and some specifics of the law in specialised areas. Conflict resolution will also often be useful training. Others will need compliance training to the extent appropriate to their duties. As with most other compliance activities, training should be properly scheduled on a periodic basis. The compliance manager will require an overview of a training program. Most training will be conducted or arranged by line management, as it will usually be directed at line functions. Involvement of the business unit’s Compliance Officer is desirable.

(A proposal for an intensive Training Program for Compliance Officers will be included here once the matter has been debated)
16 Remedial Action

16.1 Introduction
This section sets out the disciplinary procedures for employees in cases of non-compliance.

16.2 Background
Disciplined behaviour is essential both for the successful achievement of the employer’s objectives and for the safety and fair treatment of the employees. It is the responsibility of management to maintain disciplined behaviour and it is entitled to expect satisfactory conduct and work performance from employees.

For discipline to be maintained fairly the employees should know what constitutes liability as a result of misconduct and the procedures which will be followed when dealing with misconduct. A dismissal may be unfair if it is not effected for a fair reason and in accordance with a fair procedure. The facts of the case and the appropriateness of dismissal as a penalty determine whether or not a dismissal is for a fair reason.

The Labour Relations Act, 1995, recognises 3 grounds on which a termination of employment may be legitimate:
(a) the conduct of the employee;
(b) the capacity of the employee, and
(c) the operational requirements of the employer’s business.

The Labour Relations Act, 1995, further provides that dismissals for certain reasons may be automatically unfair, i.e., if it amounts to an infringement of the fundamental rights of employees and trade unions or if it is for a reason listed in section 187 of the Act such as participation in a lawful or protected strike, intended or actual pregnancy and acts of discrimination.

16.3 Disciplinary Code: Principles
A disciplinary code and procedure should be based on the following principles:
(a) Disciplinary action should be corrective as opposed to punitive, the aim being to bring about a change in the behaviour of employees who have indulged in undesirable actions so that such employees adhere willingly through greater acceptance and understanding, to standards of conduct and performance.

(b) Punitive action should only be taken when prior graduated corrective action has proved ineffectual or when a first offence is very serious.

(c) The responsibility for imposing discipline is that of management. Management must also adopt clear disciplinary rules that establish the standard of conduct required of employees. Such rules must create certainty and consistency in the application of discipline. The standards of conduct must also be clear and made available to employees in a manner that is easily understood.

(d) As far as is practicable, similar offences committed in similar circumstances will be treated equally through similar disciplinary action. Consistency in discipline is therefore of the utmost importance.

(e) Formal procedures do not have to be invoked every time a rule is broken or a standard is not met. Informal advice and correction is the best and most effective way for the employer to deal with minor violations.
work discipline. Repeated misconduct will warrant warnings which themselves may be created according to degrees of severity. More
serious infringements or repeated misconduct may call for a final warning or other action short of dismissal. Dismissal should be reserved for cases of serious misconduct or repeated offences. Generally it is not appropriate to dismiss an employee for a first offence except if the misconduct is serious and of such gravity that it makes a continuous employment relationship intolerable. When deciding whether or not to impose a penalty of dismissal, management should in addition to the gravity of the misconduct consider factors such as the employee's circumstances (including length of service, previous disciplinary record and personal circumstances), the nature of the job and the circumstances of the infringement itself. Prior to any disciplinary action being taken, careful consideration of the circumstances must be given. This must follow a thorough investigation into each incident.
17. CUSTOMER COMPLAINTS

17.1 Introduction  
Procedures and controls to accommodate customer complaints according to, *inter alia*, the Code of Banking Practice, The Financial Advisory and Intermediary Services Bill 2000 and the Policy Holder Protection Rules, are discussed in this section.

17.2 Background  
An entity must have written procedures for the effective consideration and proper handling of customer complaints and must also ensure:

(a) that each of its employees is aware of these procedures and of the obligation to follow them;

(b) a proper handling of the complaints from customers are relevant to its complaints, with the principles and the rules applicable to the conduct of that business;

(c) that any appropriate remedial action on those complaints is promptly taken; and

(d) where the complaint is not promptly remedied, the customer is advised of any further avenues for complaint available to him.

17.3 Procedure  
The procedures are mainly concerned with "significant complaints". The term significant complaint includes one which cannot be settled quickly and directly and one which involves material amounts in relation to the financial circumstances of the complaint or one which alleges:

(a) a breach of any relevant legislation;

(b) a breach of the customer mandate;

(c) bad faith, malpractice, impropriatory, repetition or recurrence of any matter about which there has been a recent complaint.

All significant complaints whether written or oral must be notified immediately to the designated officer who will be responsible for entering details of the complaint in the compliance register.

It is important that line management keep track of the complaint until it has been completely resolved.

The complaint must be considered by an officer or employee of suitable seniority (line management), who is impartial. If an impartial employee is not available, consideration should be given to obtain a suitable person outside the entity.

A letter responding to the complaint to be signed by line management should be sent to the customer without any delay. It will be sufficient to have the response reviewed by the Compliance Officer before it is sent to the complainant. Remember that even a trivial complaint if left unattended or mishandled will affect the reputation of an entity and therefore could impact
negatively on an entity.

17.4 Evaluation of the procedure
The Compliance Officer will monitor the complaint procedure according to the relevant regulatory requirement and advise on the adequacy of the complaint procedure.
The Compliance Officer will specifically monitor the following:
(a) that the complaint procedures are adequate to ensure that the complaints are properly handled; and
(b) remedial action is taken promptly and unsatisfied complainants are advised of the further avenues available to them.

It is of the utmost importance to have a proper functional customer complaints procedure in place to minimise the entity's reputation risk.
18. THE NEED FOR INDEPENDENCE

Ultimate responsibility for compliance lies with the Board of Directors. The governance structures that are in place will specify management responsibilities. The responsibility for assisting the business in complying with regulatory requirements is delegated to the compliance officer.

The Board of Directors and management will rely on the compliance function to obtain an appropriate understanding of the level of compliance with regulatory requirements.

In placing reliance on the function, they will need to know whether the compliance officer is sufficiently independent.

18.1 Why the Compliance Officer should remain independent

(a) Introduction

There is, to some degree, a natural conflict between the interests of business and complying with regulatory requirements. For instance, where management’s performance is primarily assessed on income/profit that is generated, it is likely that this is where the primary focus will remain. Compliance, on the other hand, may result in restrictions being placed on business opportunities.

(i) Why should a compliance officer remain independent?

The Compliance Officer must at all times maintain a high degree of professional independence.

This is reflected in regulation 47(1) of the Banks Act that provides that:

"A bank shall establish an independent compliance function as part of the risk management framework, in order to establish that the bank continuously manages its regulatory risk, that is, the risk that the bank does not comply with applicable laws and regulations or supervisory requirements."

If the compliance officer is not independent and reports directly to management, the compliance officer could be “captured” by management. This could be problematic if the compliance officer reports on issues of non-compliance, or where there is a conflict between business objectives and the applicable regulatory requirements.

For instance:
• Firstly, the compliance officer is reporting the failure directly to the person responsible for the failure; or
• Secondly, the report may be squashed and never reach the Board who is ultimately responsible for compliance.

The internal and external auditor functions have gone to great lengths to establish standards that promote independence. The compliance function is faced with similar challenges.
However, it is also detrimental to be too independent as the compliance officer runs the risk of becoming an "outsider." The compliance function
must ensure that it remains part of the day-to-day business decisions by assisting management in playing a role of being "part of the solution" in complying with regulatory requirements. If compliance is structured along the lines of an internal audit function, it risks being reactive rather than proactive.

This represents somewhat of a challenge in that there is a very fine line between remaining independent whilst still being part of the day-to-day business processes.

Let’s look at how the compliance reporting lines should be structured in order to ensure that there is adequate independence.

The diagram set out in Section 15 serves to highlight key aspects of reporting lines that will enhance independence. For instance, the diagram reflects the compliance officer with a direct reporting line to the chief executive officer and a direct reporting line to the Board Audit committee. This ensures that the compliance officer is sufficiently independent to perform his/her duties objectively, namely, without undue influence. In some cases, the compliance function reporting line is often to the chief risk officer. This could be structured alongside other risk functions e.g. internal audit.

(ii) Aspects of independence

In the final analysis, independence is a state of mind. In achieving this state of mind, the compliance officer should actually not only be independent but rather they should also be seen to be independent.

The compliance officer should not have any conflict of interest that would impair their independence.

Independence is central to the success of the compliance function. Without an adequate level of independence, a compliance officer would be faced with significant and perhaps fatal challenges.
19. COMPLIANCE FUNCTION REPORTING LINES

The diagram that is set out below serves to highlight compliance reporting lines that could be put in place in a large organisation:
20. CONFLICTS OF INTEREST

A conflict of interest arises when more than one stakeholder has an interest in a particular transaction.

For example, a business has a client (of 25 years standing) who is a director in a mining company and wishes to sell a portion of the company. Another client wishes to invest in mining. A situation arises where these clients have opposing interests. Whose interests come first? Can the information obtained from one client be used for the benefit of the other client?

Clearly the business should guard against committing market fraud, breaching fiduciary duties and committing insider trading offences. More importantly, there is the risk of reputational damage if any of the above was found out.

It is submitted that, if conflicts of interest cannot be avoided or adequately managed, there is a risk of going out of business.

The compliance function plays a valuable role in that it assists management to ensure that control measures are in place to avoid or manage conflicts of interest adequately.

20.1 How to Assist Management in Managing Conflicts of Interest:

(a) Introduction

Where a business holds a particular share and wishes to sell it at the highest possible price and another, a customer instructs them to purchase that particular share on his/her behalf but at the lowest possible price, a potential conflict of interest arises.

Does the trader act in the best interests of the business and sell at the highest possible price to the customer, or does he give the customer a "good deal" and prejudice the interests of the business?

Principle 8 of the Financial Services Authority's Handbook requires a firm to manage conflicts of interest fairly. The principle requires that when a conflict arises between a firm and its customer or between two customers of the firm, that the firm "pay due regard to the interest of each customer and manage the conflict of interest fairly."

Financial Services Authority — United Kingdom

Section 4 of the Collective Investment Schemes Control Act requires that a manager of a collective investment scheme must avoid conflict between the interests of that manager and the interests of an investor.

How does a compliance officer assist management to ensure that such conflicts of interest are appropriately managed?

(b) Managing conflicts of interest

Conflicts of interest may arise between:

- The interests of the business and its client;

It is acknowledged that much of the information contained in this section has been adapted from the

Compliance Institute of South Africa

Handbook for Members

March 2008
• The interests of two different clients;
• The interests of an employee and his/her employer; or
• The interests of an employee and a client.

Where possible, conflicts of interest should be avoided. However, a business may manage conflicts of interest by:
• Disclosing such interests to the customer;
• Instituting a policy of independence;
• Establishing Chinese walls; or
• Instituting a personal account trading policy.

(c) **Disclose interests to the customer**
Before a business advises a customer in respect of a transaction or deals on behalf of the customer in respect of a transaction, the business must disclose the potential conflict of interest to the customer. This should be disclosed in writing.

(d) **Institute a policy of independence**
The business may institute a policy of independence, which requires the employee to remain independent when advising or dealing on behalf of a customer, thereby representing only the interests of the customer. The business must still advise the customer that it may have a material interest. All employees must be aware of the policy.

(e) **Establish Chinese Walls**
Chinese walls are internal arrangements in terms of which information held by one person in the conduct of business is not available to persons in the conduct of another part of the business. An example of this is where traders and asset managers of the same business are prohibited from sharing information.

Is this merely a state of mind, or is physical separation required?

It is impossible to compartmentalise one’s mind. Once you are aware of information from which a conflict of interest will arise, you have been compromised. It is not possible to pretend that you don’t have such information. As a result of this, businesses often ensure that staff members such as traders and asset managers are physically separated. This can be achieved through access control whereby access to the physical office area is restricted to certain employees only, and the recording of the telephone conversations of employees located in that area.

(f) **Institute a personal account trading policy**
A personal account trading policy places restrictions on an employee trading for his/her personal account. In some businesses a complete ban is placed on personal account trading, while other businesses require prescribed procedures including prior permission from management in respect of each trade. The FSB and SARB have issued personal account trading policy guidelines.

(g) **Decline to act for a customer**
Where a business is unable to manage the conflict of interest fairly, it should decline to act on behalf of the customer.
Appropriate management of conflicts of interest is essential to maintain stakeholder confidence in a business.
21. RECORD KEEPING

21.1 Why it is Important to Keep Records

(a) Introduction
If you are asked to submit proof of an event or a transaction and you have no record thereof, how would you prove that the event or transaction actually occurred?

A business keeps records because:
- It is sound business practice to keep records of all the business that it has conducted; and
- The law requires it.

(b) For business purposes
There is obviously a need to keep records for business purposes. A business that processes numerous transactions on a daily basis must keep track of the aforementioned. This would not be possible without a permanent account of each and every transaction?

Record keeping is an important ongoing business activity.

(c) Because it is the law!
There are numerous regulatory requirements that specify that records must be kept.

Although a detailed analysis of all the regulatory requirements relating to record keeping is beyond the scope of this Handbook, some of the more significant requirements are discussed.

The following laws make it compulsory to keep records:

Regulation 47 of the Banks Act:
Regulation 47 specifically prescribes the following in respect of record keeping:

Reporting:
(c) Document the compliance officer's finding, including any remedial action, as part of the compliance-monitoring programme.

Financial Intelligence Centre Act:
Section 22 of the Financial Intelligence Centre Act prescribes that certain records in respect of business relationships and transactions must be kept for a period of 5 years, specifically:
- The identity of the customer;
- The manner in which the identity was established;
- The amount of the transaction;
- The parties involved in the transaction; and
- Any document used to verify a person's identity.

Financial Advisory and Intermediary Services Act:
The Financial Advisory and Intermediary Services Act requires that the following records be kept for a minimum period of 5 years:
- Records of advice given to customers;
- Known premature cancellations of transactions or financial products by customers;
• Complaints received, as well as an indication as to whether or not the complaints have been resolved;
• The continued compliance with the authorisation requirements of FAIS by the Financial Services Provider and the representatives; and
• Cases of non-compliance and the reasons for such non-compliance.

A financial services provider must also maintain a register of "representatives" and "key individuals" which must be regularly updated and available for inspection.

Maintenance of appropriate records will achieve an appropriate business and compliance audit trail.

21.2 The compliance activities that must be recorded

(a) Introduction
For the sake of convenience, the records that should be kept from a compliance standpoint will be discussed under the following headings:
• Compliance services
• Compliance training
• Compliance monitoring

This is not intended to be exhaustive and serves to highlight key compliance record keeping considerations.

(b) Services
In Section 7, various aspects of compliance services were considered which included the provision of advice on regulatory requirements, overseeing the implementation of the compliance process, contact with the regulators and reporting.

Each of the aforementioned is addressed below:

(i) Providing advice on regulatory requirements
The identification, analysis and prioritisation of regulatory requirements should be recorded as part of the compliance process. This will be incorporated into compliance-related documentation, for example, in risk management plans.

Copies of "regulatory briefs" or "newsletters" advising management of changes to legislation and new regulatory requirements will serve as an audit trail of the support provided to the business.

Compliance officers play an important role in providing advice on how to apply the regulatory requirements in a business context. Practical considerations relating to record keeping in this regard include the following:
• Written record of the business's request for services;
• Record of research undertaken;
• Input from regulators;
• Record of legal advice obtained;
• Record of compliance services provided; and
• Record of compliance rulings based on the business request.
Clearly judgment should be exercised in deciding when to keep records in respect of compliance services provided to management.

(ii) **Overseeing the implementation of compliance procedures**
Control measures to ensure compliance with regulatory requirements should be recorded in the risk management plans. As noted earlier, these risk management plans form part of the compliance manual.

(iii) **Reporting**
Compliance officers produce a number of reports in the normal course of their day-to-day activities. These include:
- Compliance reporting;
- Management reporting; and
- Board reporting.

Clearly copies of the reports will serve as a record of the work done by the compliance officer/function.

(iv) **Contact with regulators**
The relationship with regulators is an important aspect of the compliance function. It is essential that all significant aspects of this relationship be recorded. This includes keeping records of the following:
- Meetings held with regulators including telephonic discussions;
- Correspondence undertaken; and
- Regulatory reviews.

Copies of any and all reports to the regulator on compliance issues should be kept on file.

21.3 Training
It is good practice to keep records (attendance registers) of all employees who have attended compliance training. Where assessments of staff members that are trained are undertaken, the results of the assessment should be kept.

From a compliance perspective, this will serve as evidence of the responsibility to train staff having been fulfilled.

These records should identify who received compliance training, as well as what they received training on and the results of any assessment conducted. Record keeping provides evidence of compliance with regulatory requirements.

21.4 Monitoring
Compliance monitoring activities provide an essential understanding of how well the business is complying with the regulatory requirements.

The recording of monitoring activities is essential. The nature of the records will vary according to the type of monitoring that takes place.

The results of monitoring that is conducted should be communicated to a number of stakeholders. These include:
- Management
- Staff Members
- Internal Audit
- Risk or Audit Committees
- Board of Directors
Importantly, the results of monitoring activities should be reported to management in order to facilitate remedial action and records thereof kept on file. This serves as proof of the monitoring activities. Records of the management response to the monitoring are also important.

Compliance record keeping is essential to evidence the services, monitoring and training undertaken.
22. COMPLIANCE REPORTS

As discussed, accountability for compliance lies with the Board of Directors whilst responsibility for ensuring compliance is delegated to management.

In order to assist management and the Board, they must be adequately informed of the status of compliance. How is this achieved? One of the key means of providing the required information is through compliance reports.

22.1 Compliance Reporting to Management and the Board Of Directors

(a) Introduction

How is appropriate communication with management and the Board of Directors achieved? Particularly with respect to the status of compliance and with reference to instances of non-compliance and how these are handled?

Compliance reporting plays an important role in this regard.

(b) Compliance reporting

There are a number of regulatory requirements that require business to undertake compliance reporting.

For example, Regulation 47 of the Banks Act specifies that a bank compliance officer must submit a report on the level of compliance with laws and regulations or supervisory requirements at every meeting of the Board of Directors or the Audit Committee of the bank.

Regular reporting is essential from the lowest levels of the business through to the top levels of management and ultimately to the Board. Compliance challenges, significant events, breaches and action taken or proposed to remedy the aforementioned should be reported.

In large organisations, these reports are, in practice, rolled-up through the business. For example, from section to division to business unit to group compliance, who then submits a consolidated report to the Board of Directors.
The roll-up of reporting within large organisations is illustrated below. This is by no means the only way in which this can be structured and the illustration is only intended to demonstrate key aspects of the reporting.

The compliance reporting to management and the Board of Directors provides the necessary communication that will assist management to understand the status of compliance.
23. LIAISON WITH REGULATORS

To recap briefly on a few points:

- The primary role of the regulator is to licence businesses and then monitor and enforce compliance with regulatory requirements.
- Regulators impact on business in the following respects in that they expect business to:
  - Obtain a licence before they may conduct business;
  - Meet prudential requirements;
  - Meet the minimum standards for the conduct of business;
  - Implement compliance management systems; and
  - Report on compliance with regulatory requirements.
- Regulators also:
  - Handle complaints;
  - Monitor compliance with regulatory requirements; and
  - Take disciplinary action, which may include the imposition of fines, suspension or withdrawal of licenses.

In view of the above it is important to maintain a good relationship with regulators.

23.1 Why it is important to liaise with regulators

(a) Introduction

"You need their continuing permission in order to conduct business. You are obliged to be open and co-operative with them. They can ask you for almost any information or documentation and they can inspect your business at any time with or without notice. If they do not like what they see, your firm can be warned, fined, pilloried, ordered to pay compensation or have its profits redistributed among claimants. Ultimately, they can suspend or terminate your firm's authorization, and can prevent any individual from taking up or remaining in employment in the financial services industry in the United Kingdom and, practically speaking, in any major financial centre in the world. Neither you nor your firm can afford to incite them to action."

Newton on the role of the regulator.

The regulator holds the key that allows the conduct of business. A good relationship with the regulator is critical to the sustainability of the business in the long term. Such a relationship is only established through effective liaison with the regulator.

It is clearly advisable that business ensures that the relationship with the regulator is one of open and effective communication. In playing "open cards" with the regulator, a level of trust is developed and the business will gain a reputation of being co-operative.

The co-ordination of communication with the regulator is normally the responsibility of the compliance officer. This is the first point of contact for the Regulator with any business. The compliance officer should endeavour to be available at all times to resolve any regulatory issues that may arise. Regulators expect issues to be dealt with promptly and thoroughly.

The compliance officer is also responsible for reporting compliance issues to the regulator. For example, Regulation 47 of the Banks Act requires the
compliance officer to submit a copy of the compliance report submitted to the Board of Directors or the audit committee, to the Registrar.

Further, the FAIS Act requires the compliance officer of a financial services provider to submit an annual compliance report to the Registrar.

Experience has shown that the way in which business is viewed by the regulator, is to some extent, as a result of the nature of the relationship between the business (and in particular the compliance officer) and the regulator.
24. ACKNOWLEDGEMENTS

Regulatory requirements

References to the regulatory requirements that are imposed are made in the body of this course.

Other references

Specific references that have been used in the production of this course are set out below:


King II Report on Corporate Governance for South Africa - Institute of Directors in South Africa - March 2002


Making Ethics Work in Financial Services - Andrew Newton - 1998


The Internal Auditing Handbook - K.H. Spencer Pickett - Published by John Wiley and Sons 1999

Dynamic Auditing - Marx Van der Watt - LexisNexis Butterworths 2001

The Handbook of Compliance - Making Ethics Work in Financial Services Newton, Andrew 1998

Making Legal Compliance Work — Brian Sharpe — CCH Australia Ltd 1996

Statements of South African Auditing Standards — SAICA