Ensuring Regulatory Compliance
Integrating Risk Advisory and Assurance
In an environment where the global economic recession, demise of major financial institutions and changing business landscape has led to stricter regulations in major industries and countries around the world, the word “Regulatory Compliance” has become an all-important language that can make or mar an organisation and its directors.

Organisations are increasingly elevating the processes and structures they need to enhance compliance with regulations. The awareness of existing and new legislation applicable to an organisation as well as the implication of compliance or otherwise with the provision of each piece of legislation is a major focus area for the board.

In achieving effective Compliance Regulatory Management within an organization, the integrated roles of key management functions, mainly Legal, Compliance, Risk and Internal audit must be understood and enabled.

Understanding the Regulatory Universe of the Organisation
With over 300 pieces of legislation in South Africa, the legislation applicable to each organisation will vary from one to the other depending on the type of industry and the nature of the organisation and its business imperatives. Every organisation has a responsibility to identify existing and emerging legislation relevant to its business and ensure that risks that may arise from the compliance requirements are well understood by the board and management.

The risks that may stem from non-compliance with key legislative requirements can be very costly and damaging to an organisation and the custodians of governance within the organisation. The consequences of non-compliance range from penalties and fines, to imprisonment, withdrawal of licenses, lawsuits and reputational risk which may individually and or collectively have a fundamental impact on the organisation’s sustainability as a going concern; as well as the impact that a lack of good corporate governance at board and business levels can have on the business.

The impact and probability of the risks that the legislation represents depend on the attention paid to the legislation and how well risk and compliance management is entrenched within the organisation. It is therefore critical that an organisation implements relevant structures and processes to effectively manage and monitor the compliance process to ensure that these are entrenched in a way that compliance becomes “second nature”.

When new legislation is promulgated, the inherent risk will always be high (red) as operational breakdowns have a high probability/likelihood of occurring in the business.
Roles and Responsibilities around Regulatory Compliance Management

Embedding compliance with all key legislation in the organisation is a function of certain critical activities and stems from collaboration across key functions such as Legal, Compliance, Risk Management, Business and Internal Audit. These functions all form part of the “three lines of defence”.

**Identifying the three lines of defence**

The success of any compliance management and monitoring programme depends on the existence, functioning and integration of these lines of defence in the performance of their duties. These three lines of defence as well as an overview of their key responsibilities are depicted in the diagram below:

---

**1st line of defence - Management Assurance**
- Assists in setting and executing strategies.
- Provides direction, guidance and oversight.
- Promotes a strong risk culture & sustainable risk return thinking.
- Promotes a strong compliance culture and management of risk exposure.
- Ongoing monitoring and management of risks.

**2nd line of defence - Risk Management, Legal & Compliance**
- Formal, robust and effective risk management within which the organisation’s policies and minimum standards are set.
- Objective oversight and the ongoing challenge of risk mitigation, management and performance while reporting is achieved across the business units.
- Overarching risk oversight across all risk types.

**3rd line of defence - Internal Audit & other Independent Assurance Providers**
- Independent and objective assurance of overall adequacy and effectiveness of governance, risk management and internal controls within the organisation as established by the 1st and 2nd lines of defence.
- Ability to link business risks with established processes and provide assurance on the effectiveness of mitigation plans to effectively manage organisational risks.
1.1. Legal / Compliance
An organisation may decide to have its Legal and Compliance functions integrated or operating as two separate units. This is usually done with consideration for the complexity, size and structure of the business. A Compliance Officer does not necessarily need to have a legal background, while this is a prerequisite for a Legal Officer, he/she will also handle litigation.

It is the responsibility of the Legal/Compliance function to stimulate and train the board and management on legislation pertinent to the organisation. The Legal and/or Compliance function should undertake the following:

• Compile and maintain a legislative universe for the organisation.
• Facilitate the risk prioritisation of all pieces of legislation in the regulatory universe. This should be done working together with the Risk Management division and using the organisation’s risk management framework.
• Initiate new legislative requirements within the organisation. Review the legislation to confirm whether it affects the organisation, and how.
• Analyse and send out alerts on the new law to inform the organisation of the new requirements.
• Facilitate an executive review of the legislation by Legal analysts.
• Facilitate the completion of the Compliance Risk Management Plan (“CRMP”) – Interpret key legislation in plain language on the CRMP and ensure the identification of issues, controls, risk exposure, responsible parties and monitoring plans by other participating parties such as Business and Internal Audit.
• Update compliance monitoring plans on the CRMP.
• Escalate compliance matters to management.
• Undertake quarterly compliance reporting.

1.2. Risk Management
The Risk Management function should support the Compliance Office with the risk rating of the relevant legislation once such legislation becomes operational in the business. A compliance risk register for the regulatory universe, showing both the inherent and residual ratings of each piece of legislation, based on impact and likelihood, should be the product of this process.

The penalties - financial, imprisonment, etc - and other business risks associated with key provisions of the legislation should be identified and captured on the compliance risk register for the regulatory universe as management should know if a piece of legislation will affect shareholder value.

The knowledge of associated penalties triggers management to provide the resources and budget needed for the implementation of compliance requirements.

1.3. Business Operational Compliance
Once the Legal / Compliance function has effectively identified and interpreted compliance requirements and facilitated the risk ratings on the Compliance Register, Business is responsible for ensuring the implementation of such compliance requirements.

The Business should identify any key issues that may arise from the compliance requirements and capture these on the CRMP for monitoring and report-back to relevant structures and the board.

Business should have its own Business Operational Compliance Officer / Champion who, upon receipt from the Legal / Compliance Officer, the information pack containing the executive review, compliance alert, CRMP and presentation material, will commence the operational monitoring of the compliance of business processes to the legislative requirements.

Again, depending on the size and maturity of the organization, the roles of Legal / Compliance Officer can be combined with that of the Business Operational Compliance Officer, even that of the Risk Officer. This, of course, should be with due consideration of the nature and magnitude of business operations, the risk profiles as well as the cost and benefits of combining or separating the functions.

Business should readily be able to provide Internal Audit with the legislative universe of the organisation for the commencement of a compliance audit.
1.4. Internal Audit

Internal Audit, as the assurance provider, is responsible for reviewing the adequacy and effectiveness of the functioning of controls implemented by management to ensure compliance with legislative requirements. In conducting a review of compliance within the organisation, Internal Audit should ask the following questions:

- What are the pieces of legislation that should be reviewed?
- What new processes are being put in place as a result of compliance requirements?
- What new systems are being put in place to support and monitor compliance?

The span of the internal audit review will be: Legislation – Policy – Procedures – Systems / Processes. Internal Auditors should be able to map the legislation to the existence of a policy and a risk map. They need to substantiate and audit compliance risk ratings that have changed, especially where residual ratings show improved controls. For example, if the organisation has had many complaints escalated to an ombudsman, it is a likely indication of non-compliance and hence the applicable residual rating cannot be acceptable (green); it should probably be yellow or red.

From their review, Internal Auditors should be able to validate or provide the following inputs to the CRMP:
- Impacted Areas – processes, systems and policies
- Existing Controls
- Additional Controls – arising from amendments to, or new, legislation
- Risk Exposure – High, Medium, Low
- Responsible Party – Affected Parties
- Monitoring Plan – Business Unit Compliance

A short interpretation of the integrated role of the functions is shown in the diagram below:
Compliance Certifications

As mentioned above, a legal background is not mandatory for a Compliance Officer but he/she should possess the relevant competence to effectively manage compliance with the relevant pieces of legislation for the organisation. Acquiring the relevant compliance certification may be a good start and an added advantage.

An internal Auditor is ideally well positioned to assess the adequacy and effectiveness of management’s controls over regulatory compliance; however, some organisations may decide to further upskill their internal auditors on specific compliance areas by requiring them to undergo particular relevant certification programmes.
A view of the Regulatory Universe of Key Industries

Below is an overview of key pieces of legislation, relating to specific industries:

- Auditing Profession Act 26 of 2005
- Banks Act 94 of 1990
- Basic Conditions of Employment Act 75 of 1997
- Broad-Based Black Economic Empowerment Act 53 of 2003
- Companies Act 71 of 2008
- Compensation for Occupational Injuries and Diseases Act 130 of 1993
- Constitution of the Republic of South Africa of no 108 of 1996
- Consumer Protection Act 68 of 2008
- Customs and Excise Act 91 of 1964
- Deeds Registries Act 47 of 1937
- Development Bank of Southern Africa Act 13 of 1997
- Electronic Communications Act 36 of 2002
- Employment Equity Act 55 of 1998
- Environment Conservation Act 73 of 1989
- Exchange Control Amnesty and Amendment of Taxation Laws Act 12 of 2003
- Financial Advisory and Intermediary Services Act 37 of 2002
- Financial Institutions (Protection of Funds) Act 28 of 2001
- Financial Intelligence Centre Act 38 of 2001
- Financial Services Board Act 97 of 1990
- Hazardous Substances Act 15 of 1973
- Income Tax Act 58 of 1962
- Labour Relations Act 66 of 1995
- Liquor Act 59 of 2003
- Municipal Finance Management Act no 56 of 2003
- Municipal Systems Act 32 of 2000
- National Environmental Management Act 107 of 1998
- Occupational Health and Safety Act 85 of 1993
- Patents Act 57 of 1978
- Preferential Procurement Policy Framework Act 5 of 2000
- Prevention of and Treatment for Substance Abuse Act 70 of 2008
- Promotion of Access to Information Act 2 of 2000
- Public Audit Act, no 25 of 2004
- Public Finance Management Act no 1 of 1999
- Public Investment Corporation Act 23 of 2004
- Reinsurance of Damage and Losses Act 56 of 1989
- Securities Services Act 36 of 2004
- Short-term Insurance Act 52 of 1998
- Skills Development Act 97 of 1998
- Tobacco Products Control Act 83 of 1993
- Unemployment Insurance Act 63 of 2001
- Value-Added Tax Act 89 of 1991

...
Conclusion

With the current business landscape, where legislation emerges and changes continuously with increasing requirements to keep business on the right track, it is critical for every organisation to implement adequate and effective structures to embed a culture of compliance.

Internal Auditors must take responsibility to become familiar with the legislative universe of their organisations and assist in providing assurance that structures and processes are adequate and effective to mitigate compliance risks.
Contacts

Dave Kennedy
Service Line Leader – Risk Advisory
Deloitte South Africa
Cell: +2782 780 9812
Email: dkenney@deloitte.co.za

Pramesh Bhana
Director – Risk Advisory
Deloitte South Africa
Cell: +2782 303 2227
Email: pbhana@deloitte.co.za

Mark Victor
Director – Risk Advisory
Deloitte South Africa
Cell: +2782 772 3003
Email: mvictor@deloitte.co.za

Kriba Moodley
Associate Director – Risk Advisory
Deloitte South Africa
Cell: +2783 327 4500
Email: kmoodley@deloitte.co.za

Dean Chivers
Director – Risk Advisory
Deloitte South Africa
Cell: +2782 415 8253
Email: dechivers@deloitte.co.za

Bukkie Adewuyi
Senior Manager – Risk Advisory
Deloitte South Africa
Cell: +2776 4050 465
Email: aadewuyi@deloitte.co.za

Munier Damon
Director – Risk Advisory
(Cape Town)
Deloitte South Africa
Cell: +2783 2342 336
Email: mdamon@deloitte.co.za

Navin Sing
Director – Risk Advisory
(Kwazulu Natal)
Deloitte South Africa
Cell: +2783 304 4225
Email: navising@deloitte.co.za

Jens Kock
Director – Risk Advisory
(Namibia)
Deloitte Namibia
Cell: +2648 1124 5457
Email: jkock@deloitte.co.za

Regional Contacts

Mark Victor
Director – Risk Advisory
Deloitte South Africa
Cell: +2782 772 3003
Email: mvictor@deloitte.co.za

Navin Sing
Director – Risk Advisory
(Kwazulu Natal)
Deloitte South Africa
Cell: +2783 304 4225
Email: navising@deloitte.co.za

Jens Kock
Director – Risk Advisory
(Namibia)
Deloitte Namibia
Cell: +2648 1124 5457
Email: jkock@deloitte.co.za