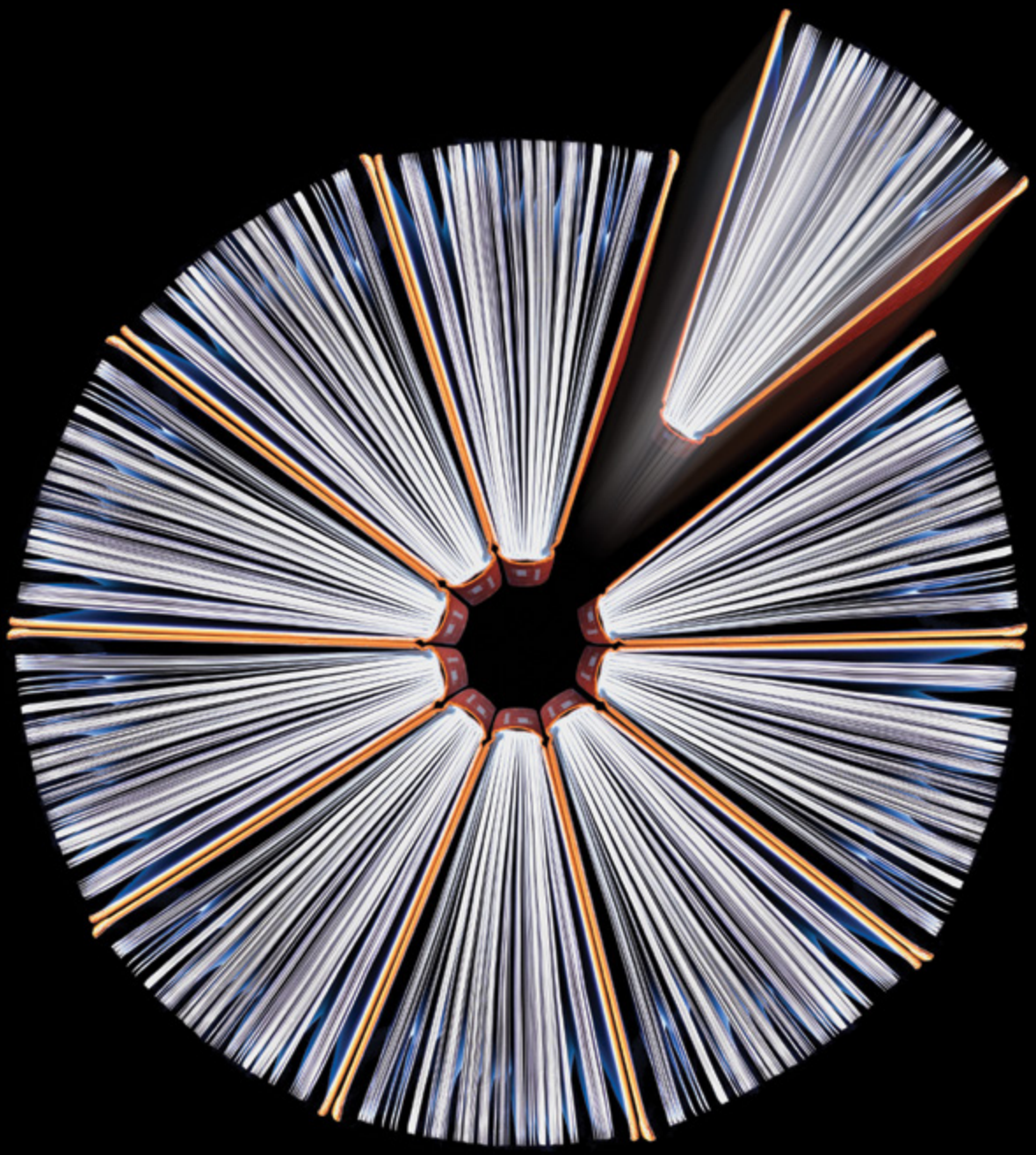
Deloitte.



Ensuring Regulatory Compliance

Integrating Risk Advisory and Assurance

Contents

Introduction

In an environment where global economic challenges, increased pressure on major financial institutions and changing business landscapes have led to stricter regulations in most major industries and countries around the world, the phrase “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 increased business impact of new legislation as well as the implications of non-compliance within each organisation means the provision of applicable legislation has increased the focus by the board on regulatory compliance.

In achieving effective Regulatory Compliance Management (RCM) within an organisation, the integrated governance roles of key management functions, mainly Legal, Compliance, Risk and Internal Audit must be understood and enabled.

Understanding the Regulatory Universe of the Organisation

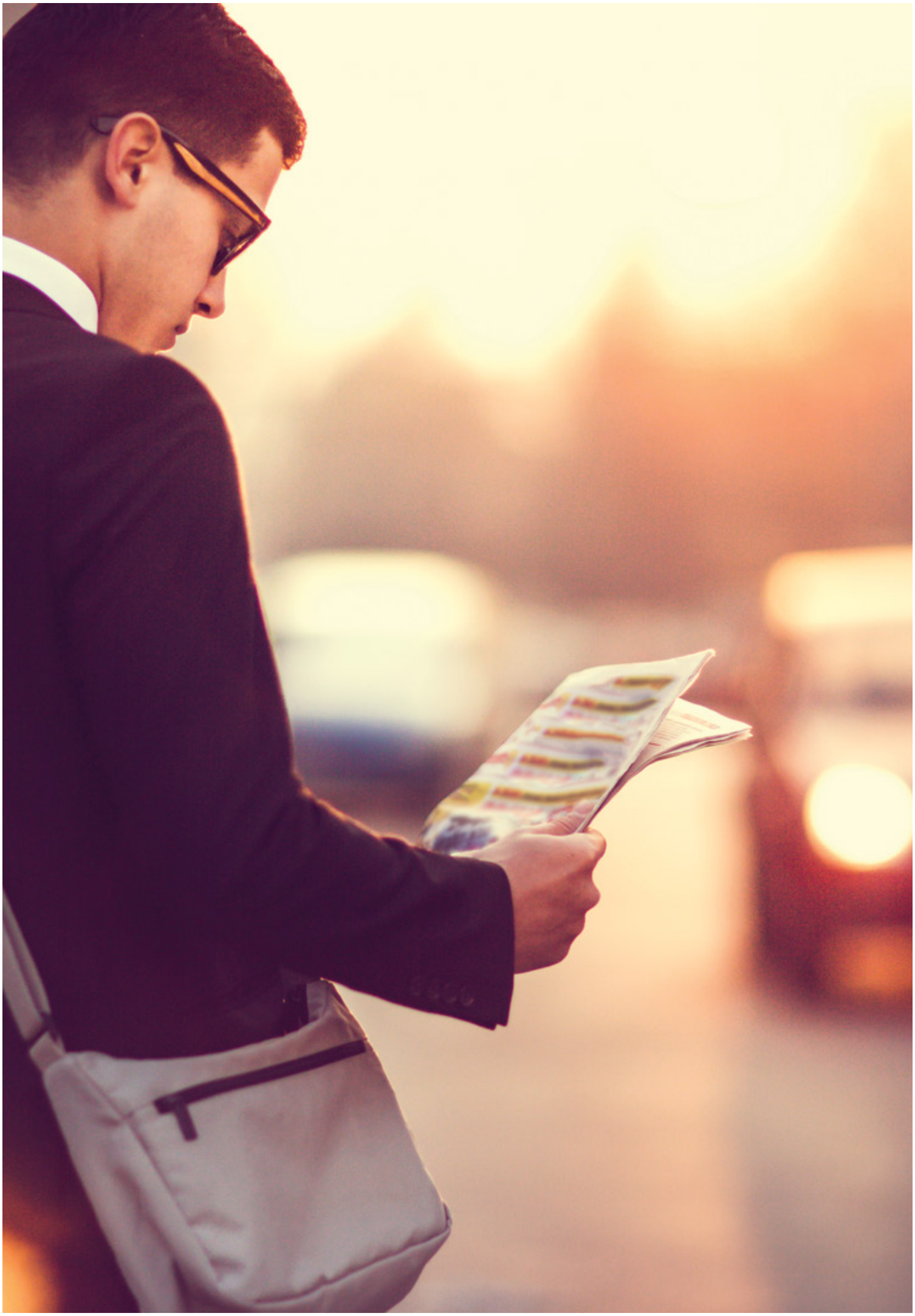
With over 500 pieces of legislation in South Africa, the legislation applicable to each organisation will vary from one to the other, depending on the type of industry, the nature of the organisation and its business imperatives. Every organisation has a responsibility to identify existing and emerging 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, litigation 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 organisation.

The impact and probability of the risks that the legislation represents depend on the attention paid to the legislation and how well risk and RCM 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 embedded in business as usual processes.

Residual risk related to all legislation will remain high until the organisation is able to implement measures or controls that effectively mitigate the risks arising out of compliance requirements, especially in respect of new legislation.

When new legislation is promulgated, the inherent risk will always be high as operational breakdowns have a higher probability/likelihood of occurring in the organisation.

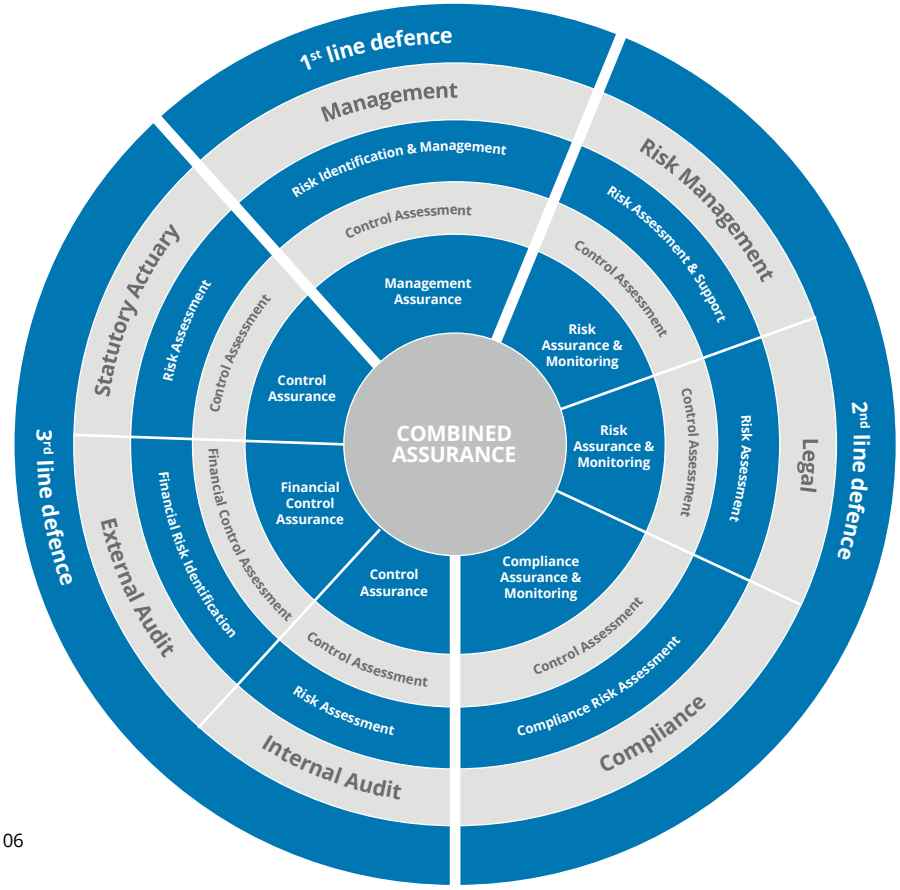


Roles and Responsibilities around Regulatory Compliance Management

Embedding compliance with all key legislation in the organisation is a function of certain critical activities and stems from collaboration across key governance functions such as Legal, Compliance, Risk Management, and Internal Audit. These functions all form part of the "three lines of defence". Business and its operational management however also form a critical (if not the most important) line of defense in ensuring a "compliant" organisation.

Identifying the three lines of defence

The success of any RCM 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 and sustainable risk-return thinking
- Promotes a strong compliance culture and management of risk exposure
- Implements control design
- Ongoing implementation of controls and management of risks

2nd line of defence – Risk Management, Legal and Compliance

- Formal, robust and effective risk management within which the organisation's policies and minimum standards are set
- Interpretation of regulatory compliance requirements
- 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
- Regular monitoring of Risk, Legal and Compliance
- Ongoing Risk, Legal and Compliance advise to the 1st line of defence

3rd line of defence – Internal Audit and 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

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 organisation. 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. Legal training is advantageous when it comes to interpreting statutes and contracts related to regulatory compliance.

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 regulatory universe for the organisation
- Facilitate the risk prioritisation of all pieces of regulation in the regulatory universe. This should be done working together with the Risk Management team and using the organisation's risk management framework
- Initiate projects to comply with new regulatory requirements within the organisation. First it is necessary to review the regulation to confirm whether it affects the organisation, and how
- Analyse and send out alerts on new regulation to inform the organisation of the new requirements
- Facilitate an executive review of the regulation by Legal analysts.
- Facilitate the completion of the Compliance Risk Management Plan ("CRMP") – by interpreting key legislation in plain language on the CRMP and ensuring 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 regular compliance reporting

Risk Management
The Risk Management function should support the Compliance Office with the risk rating of the relevant regulation once the requirements of such regulation become operational in the organisation. A compliance risk register for the regulatory universe, showing both the inherent and residual ratings of each piece of regulation, 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 regulation should be identified and captured on the compliance risk register for the regulatory universe as management should know if a piece of regulation will affect shareholder value. The knowledge of associated penalties triggers management to provide the resources and budget needed for the implementation of compliance requirements.

Business should have its own Business Operational Compliance Officer/Champion who, upon receipt from the Legal/ Compliance Officer, of 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 organisation, 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, segregation of duties, the risk profiles as well as the cost and benefits of combining or separating the functions.

The Business should identify any key issues that may arise from compliance requirements and capture these in CRMPs which can form critical management, monitoring and reporting tools if designed and implemented correctly.

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.

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

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 regulatory requirements. In conducting a review of compliance within the organisation, Internal Audit should ask the following questions:

- What are the pieces of regulation 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: Regulation – Policy – Procedures – Systems/Processes. Internal Auditors should be able to map the regulation 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, regulation
- Risk Exposure – High, Medium, Low
- Responsible Party – Affected Parties
- Monitoring Plan – Business Unit Compliance

A high level interpretation of the integrated role of the functions is shown in the diagram below:

Legal Operational Compliance

- Maintain and update regulatory universe
- Educate management and board on regulatory interpretation & requirements
- Facilitate regulatory risk prioritisation
- Maintain CRMP
- Assist business with implementation of operational compliance
- Monitor & report compliance matters

Internal Audit

- Assess adequacy and effectiveness of compliance processes, systems & structures
- Highlight key weaknesses and associated risks noted and make recommendations to management & board on corrective actions

Risk Management

- Conduct regulatory risk prioritisation
- Facilitate completion of compliance risk-register with ratings and mitigating actions
- Ensure awareness on the part of management & board on risk consequences of non-compliance

A view of the Regulatory Universe of key 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 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 53 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

Navin Sing
Managing Director: Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navising@deloitte.co.za

Dean Chivers
Risk Advisory Africa Leader: Governance, Regulatory & Risk
Mobile: +27 82 415 8253
Email: dechivers@deloitte.co.za

Candice Holland
Director: Risk Advisory Southern Africa
Mobile: +27 82 330 5091
Email: caholland@deloitte.co.za

Anthony Smith
Director: Risk Advisory Southern Africa
Mobile: +27 83 390 6757
Email: asmith@deloitte.co.za

Julie Akinyi Nyangaya
Risk Advisory Regional Leader: East Africa
Mobile: +254 72 011 1888
Email: jnyangaya@deloitte.co.ke

Tricha Simon
Risk Advisory Regional Leader: Central Africa
Mobile: +263 867 700 0261
Email: tsimon@deloitte.co.zm

Anthony Olukoju
Risk Advisory Regional Leader: West Africa
Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

Deloitte.

Designed and produced by Creative Services at Deloitte, Johannesburg.
(812231/jar)