CGF RESEARCH INSTITUTE (PTY) LTD
Corporate Governance Framework®

ARTICLE

Johannesburg
02 February 2017

ARE YOU READY FOR REGULATORY ONSLAUGHT AND INTERVENTIONS?

By Lucien Caron and reviewed by Terrance Mark Booysen

Increasingly, large and small organisations are under mounting pressure to manage regulatory compliance and their associated risks more effectively. Greater attention thus needs to be given to the organisation's risk appetite and its risk mitigation, both at the enterprise and service-line levels.

Regulatory audits have confirmed that regulatory compliance is underpinned by the quality and integrity of data and the management thereof - getting it wrong could prove very costly. In this regard, the cost of poor compliance is usually both financial and reputational as demonstrated recently by the record fines imposed on a number of South African organisations by regulators.

The rate of regulatory change is extremely high

Over the last month there have been 89 new regulatory changes introduced by various regulators, the bulk of which will apply to all organisations in South Africa. The list of affected areas include, amongst others, the following:

Affected area	Number of changes
Tax	17
Employers/Employees	8
Financial Services	8
Company and Corporate	5
Municipal By-Laws	5
Black Economic Empowerment	4
Medical Aid	4

In the same period, other regulatory changes include those found in environmental law (3), stock exchange law (3), telecommunications law (3), anti-money laundering law (2), banking law (2), competition law and consumer protection law.

Regulators are changing their approach

An interesting development in managing regulatory risk is the change in the approach adopted by regulators. Gone are the days of regulators accepting a mere 'tick box' approach to managing regulatory risk. This approach was replaced by a more customer-centric approach called *"treating customers fairly"* which is evident in legislation such as the Consumer Protection Act, 2008 and the Protection of Personal Information Act, 2013 ('POPI'). POPI is expected to be enacted soon and it has wide ranging impacts across many business areas of any South African based organisation.

The approach of regulators has evolved further since the "treating customers fairly" concept to now also include a broader approach, loosely termed the *"conduct risk"* approach and its consequent management. Briefly put, conduct risk management is the ability of an organisation to identify potential risks that would negatively impact on customers and the embedment of the principles of treating customers fairly - both within the business and within outsourced services.

Regulators have indicated that they will be testing whether organisations are managing their conduct risk effectively by, for example, reviewing an organisation's existing regulatory frameworks, testing the effectiveness of their operational embedment of the treating customers fairly principles and incorporating these principles into legislation such as those afore-mentioned. In addition, regulators have also outlined the various areas of business that will be scrutinised to test effective regulatory risk management. These principles include, amongst others, evaluating the culture and governance of an organisation, unfair contract terms, misleading advertising and marketing, ineffective and/or misleading disclosures, conflicting advice, poor claims handling and poor complaints handling. The overriding methodology that regulators will adopt in examining these areas is to test outcomes rather than adopting a mere compliance 'tick box' approach.

Within the financial services sector, regulators have commenced their testing of these principles and they have found many common problems amongst organisations in their investigations. These include:

- an insufficient capacity and level of skill within the organisation's compliance function;
- poor organisational insight pertaining to the organisation's strategic and operational impact of regulatory developments;
- a lack of integration of regulatory risk into the organisation's enterprise risk management framework;
- inadequate focus on conduct issues by internal audit which tends to be largely financial and process focused; and
- a lack of understanding of conduct risk issues.

What is the cost of non-compliance?

Regulators are inclined to use a variety of methods to penalise organisations for regulatory non-compliance, some of which include:

- monetary fines which, while still significant and growing, can be the "least of the costs" imposed on an organisation or individual. The financial implications are generally much wider than the actual fine levied and the organisation's reputation may also be adversely affected. Moreover, the penalties may include the prohibition or restriction on the selling of certain products or ultimately the closure of the organisation itself;

- regulatory action which can negatively impact the perceptions of the organisation's investors and result in a negative impact on the organisation's share price;

- directors and senior managers increasingly being held personally accountable for their own behaviour, which can thwart and even end their careers by way of criminal convictions;

- expensive and disruptive operational consequences caused by non-compliance, including the increased cost of recruiting and retaining high-quality compliance resources to remedy the situation. Instead of focusing on the business of doing business, the remedial actions required to become compliant inevitably cause massive business distractions, not least of which may include wasted time, money and resources.

In most cases it is not the fines, penalties or threat of imprisonment that will drive organisations toward regulatory compliance; understandably organisations are mostly concerned about maintaining their reputation and so their compliance in this regard is driven by the need to safeguard their reputation. Generally, the cost of reputational damage caused by non-compliance with regulatory demands far outweighs the associated fines and penalties. Getting these critical matters wrong can, and has, proven fatal to the very existence of many organisations.

How should you manage your regulatory risk?

In terms of good governance principles and practices, the organisation should ensure that:

- the board and executive management are familiar with the organisation's regulatory requirements and that these are augmented within the organisation's Corporate Governance Framework®;
- management is responsible for the implementation and execution of effective regulatory compliance management;
- there is a strong and robust oversight of the organisation's compliance management;
- there is continual monitoring of the regulatory environment which has bearing upon the organisation and its supply chain and there are appropriate responses to the applicable regulatory changes;
- there is independent assurance on the effectiveness of compliance management; and
- there is adequate reporting on compliance management both internally and to the relevant external stakeholders.

For an organisation to be able to meet the demands of regulatory compliance, it will need to ensure that there is accurate and qualitative data that underpins all the organisation's records and activities in a manner which clearly demonstrates effective and proactive regulatory risk management. Such data management disciplines will enable the board to report accurately and comprehensively to all stakeholders, including regulators.

ENDS

Words: 1,071

For further information contact:

CGF Research Institute (Pty) Ltd
Terrance M. Booysen (Chief Executive Officer)
Tel: 011 476 8264
Cell: 082 373 2249
E-mail: tbooysen@cgf.co.za
Web: www.cgf.co.za

Lucien Caron (lead Independent Consultant)
Tel: 011 476 8264
Cell: 082 787 7010
E-mail: lucien@corporateadvisory.co.za