national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

Public Sector Risk Management Framework

Reporting Lines

1 Introduction

Many institutions have difficulty in deciding the correct reporting lines for the risk management function. The main reason for this is that risk management embraces most aspects of the institution, such as strategy, finance, human resources, service delivery and public relations. In addition, the risk management function has close links to activities such as insurance, compliance, governance, internal audit and loss prevention. It is therefore understandable that the reporting lines for risk management are not immediately apparent.

The reporting line of the Chief Risk Officer (CRO) is not prescribed in the public sector risk management framework nor is there a common blue print for how this dilemma can be addressed. This creates flexibility for institutions to determine the appropriate placement of the CRO in the institutional hierarchy.

2 Guiding principles

In ideal circumstances the CRO should report directly to the Accounting Authority / Officer (AA/AO) given the latter's legal responsibility for risk management. However, where this is not practical because of the AA/AO's large span of control and other operational factors, the AA/AO should delegate on the basis of the following principles:

- The CRO should enjoy sufficient "power of office" such that his/her influence does not become diluted, conscious of the fact that the CRO needs to work with and through top management;
- The person that the CRO reports to is at a sufficiently high level in the institution (preferably not more than 1 level below the AA/AO) and is able and willing to provide the necessary direction, support and guidance to the risk management function;
- Regardless of who the CRO reports to, it is clear throughout the institution that the risk management function is an institutional resource and not an extension of the function under which it is placed for reporting purposes;
- The CRO should have a dotted reporting line to the Risk Management Committee.

2.1 The need for a separate risk management unit

Once again there is no formula for deciding upon the need for and size of a separate risk management unit. Factors to consider in this regard are:

- The current versus the desired risk management maturity level;
- The degree of risk management expertise within the existing management structures;
- The capacity within the existing management structures to absorb the additional workload;
- Resources required to effect the change within the required timeframe.

Experience has shown that it is normal to have a relatively high need for increased resources during the initial phase of the ERM implementation, with a reduced need over time, as maturity levels increase and more of the work is embedded in the core management activities.

For example initial tasks could include time consuming and labour intensive tasks such as the development and implementation of ERM framework, facilitation of risk assessment workshops, risk awareness, governance reports, loss data analyses, integration with safety management, insurance duties and many others.

2.2 Alternatives

If the budget or manpower plan does not allow for a full-time risk management department then other alternatives should be considered.

For example, one approach is to appoint one full-time CRO who uses a spread of management support and consultants to complete the risk management tasks.

Another alternative would be to outsource the risk management coordination to an independent consultant who works under the accountability of an executive member of management.

The question often arises as to whether an existing compliance officer or internal auditor may take on the responsibilities of a CRO. The International Standards for the Professional Practice of Internal Auditing allows for internal Audit to be involved in risk management; however this activity should be independently audited by another party. The test for independence is simple. If the CRO has functional responsibility such as health and safety, insurance and security, this cannot be performed by internal audit. If the CRO facilitates risk management processes, and has no decision making authority, internal audit can perform the function. The risk management function can be allocated to another member of management that has sufficient skill, capacity and standing to effect the activities required. It is more important that the function is actually performed, than deciding who should deliver this.

The role of independent assurance is mostly performed by compliance and audit staff rather than a CRO. Some allowance for organisational differences can be made but the general principle of separating the management of risk and the assurance of controls should be maintained.

Click here to see examples of possible risk management structures.