Deloitte.

Governance and Culture of Risk Management in Namibian Organisations

April 2020

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Background

Organisations in Namibia are vulnerable to various internal risks, ranging from non-compliance with laws and regulations and breaches in cybersecurity to non-adherence to day to day business procedures, among others.

Furthermore, entities are also vulnerable to external risks. The current major external risks affecting most organisations in Namibia are the trending economic recession coupled with the recent global pandemic, COVID-19. The African Economic Outlook 2020 highlighted that the Namibian real GDP peaked at 6.1% in 2015 but declined by an estimated 0.5 % in 2018 and a further 1.0% in 2019. This was partly caused by government fiscal consolidation to correct growing imbalances from high public spending and falling revenues from the Southern African Customs Union (SACU)[1].

External risks known as "black swan" risks, with low likelihood of occurring but catastrophic impact on organisations when they materialise, such as the current COVID-19 crisis, are testing how agile Namibian organisations really are. This has necessitated an evaluation of organisations' risk governance and culture in dealing with an evolving and fluid risk landscape.

This article aims to give an insight on the governance and culture of risk management in organisations in Namibia by leveraging off the 2019 Deloitte Corporate Governance survey ("survey") results.

1. Introduction

It is crucial that organisations are effective in managing risk. The Corporate Governance Code for Namibia ("NamCode") states that the board should take responsibility for the governance of risk through exercising its leadership in preventing risk management from being a series of activities that are detached from the realities of the company's business.

Aside from the board's oversight duties of risk management, for effective governance of risk, two crucial elements should be in place as per NamCode:

- An approved risk management policy and plan should be documented and widely distributed throughout the company, which sets the tone, top down, for risk management in the organisation. This is an imperative document as it is the cornerstone of *governing risk* and setting the *culture around risk* in an organisation.
- The board should have assistance to discharge its risk duties and responsibilities through the appointment of a risk committee or an audit committee that may review the risk strategy and delegate its execution to management.

It is also imperative that a positive risk management culture is inculcated at all levels in the organisation. This translates to risk management being embedded into all spheres of the organisation including strategy and projects.

[1] https://www.afdb.org/en/documents/african-economic-outlook-aeo-2019-english-version

2. Governance of Risk Management

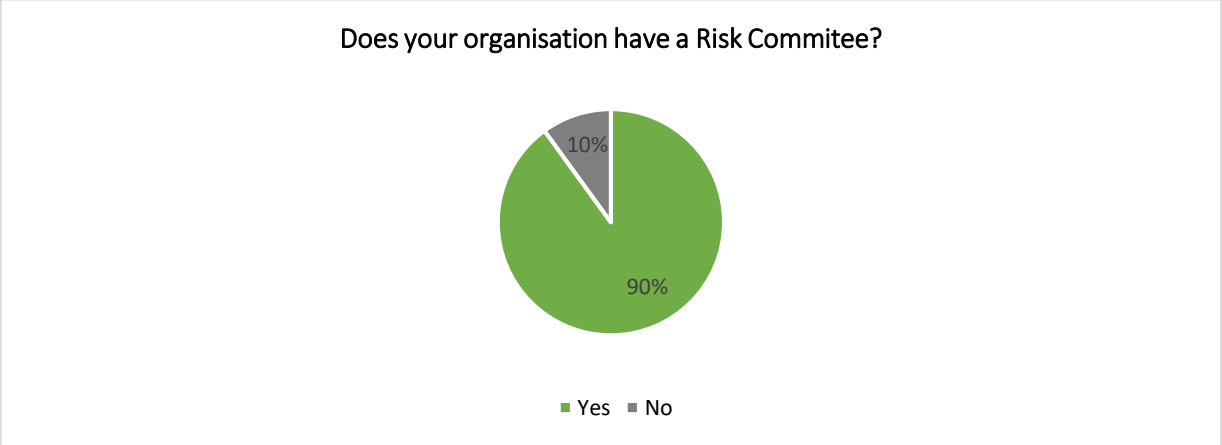
The board is responsible for the governance of risk. For the board to effectively carry out its responsibilities, it should delegate the implementation and execution of the risk management function.

Risk Committees in Namibia

NamCode states that organisations in Namibia should have a risk committee or audit committee to assist the board in carrying out its risk responsibilities. The survey revealed that:

- In relation to board structures, 10% of organisations in Namibia do not have a distinct risk committee in place, however all the organisations revealed that they have an audit committee.

- Risk oversight is coordinated through various platforms and activities as highlighted below (more than one option was selected):



This reveals that governance structures could be improved to enhance the effectiveness of the board in respect of risk governance. The risk oversight function should be allocated to a specific committee, such as the Audit and Risk or Risk and Compliance Committee that reports into the board. Detailed risk discussions should be held at the nominated committee to resolve any issues that may arise. This may particularly be useful in times where organisations need to manage crises, such as COVID-19. This will enable the response to crises to be seamless if the governance structures in place are sound. The board may also provide critical communication in relation to pervasive risks or may delegate these to management.

NamCode recommends a minimum of 3 members on a risk committee or its equivalent. The survey revealed that:

- 11% of organisations in Namibia have 2 members on the committee, 1 person less than the best practice recommended by NamCode.

Organisations with two members may find it difficult to attain a quorum, which thus delays and impacts decision-making. This may also limit the contributions to be made due to limited diversity of thought.

NamCode recommends that the risk committee meetings should at least be bi-annual. The survey revealed:

- That 70% of audit and risk committees meet more than 4 times per annum, 25% meet at least 3 times per annum, whilst the remaining 5% meet more than 7 times per annum respectively.
- Only 13% of organisations in Namibia discuss most significant risks to the organisation annually, which is insufficient. 4% do not have these discussions on their agenda and 22% do not know about these discussions.

The frequency of the committee meetings is sufficient. However, there is a need for the full board to discuss the most significant risks of the organisations more frequently. This may assist boards to make decisions by taking unpredictable risks into account or doing scenario planning. Risk should be a standing agenda at board meetings and enough time should be devoted to it.

3. Culture of Risk Management

Culture consists of the attitudes, behaviours and understanding about risk, both positive and negative, that influence the decisions of management and personnel as per the COSO Enterprise Risk Management Framework[2].

The survey revealed the following series of activities relating to risk exposures that are impacted by the culture of risk in organisations:

[2] https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf

3.1 Cybersecurity breaches

Compliance with laws and regulations is an area prone to risk in organisations. An array of organisations in Namibia, predominantly entities in the financial services industry, who have been impacted by digital disruption are vulnerable to security breaches, i.e. cybersecurity breaches.

The survey revealed the following regarding cybersecurity:

- 31% of organisations in Namibia have a low level of awareness of cybersecurity and 9% still do not know about cybersecurity. The remaining 59% has a moderate to high level of awareness.
- A repercussion of low-level cybersecurity awareness is that 36% of organisations in Namibia have experienced a cybersecurity breach within the past 2 years and 18% of organisations are not aware of these occurrences.
- 10% of organisations in Namibia do not have a committee that oversees cybersecurity issues.

According to the Checkpoint research in 2019, Namibia is the most targeted country in Africa on cybercrime[3]. It is imperative therefore that robust governance structures are implemented and a positive risk culture is inculcated to mitigate risks including those related to cybercrime. This will assist organisations to be proactive, invest in risk management and build rigorous systems and controls.

In addition, organisations should constantly monitor and evaluate risks that are constantly evolving. It is also critical to constantly examine new regulatory requirements that may impact organisations' operational efficiency.

These structures, risk culture and monitoring of cyber risks will assist Namibian organisations to manage new risks, such as the increase in cyber-attacks during the COVID19 pandemic. These attacks are luring people into opening phishing emails through social engineering. Rigorous systems will validate that organisations are operationally resilient even during a crisis and that they are able to comply with the necessary laws and regulations.

3.2 Brand Reputation and the Review of Ethical Breaches

7% of corporate entities in Namibia do not periodically review protocols in place that deal with ethical breaches, such as deceptive tactics, human rights, fines among others, and neither do they evaluate the associated risks on brand reputation.

It is imperative that organisations review and address any ethical breaches detected. It is then crucial to implement protocols and detective systems that will assist with detection of ethical breaches. Consequence management should be implemented to deter unethical behaviours that may tarnish the reputation of the organisation. A positive brand reputation should always be evaluated and maintained.

[3] https://itweb.africa/content/mQwkoq6PA9973r9A

4. Conclusion

The governance and risk culture of organisations in Namibia needs to be improved. It is necessary to establish appropriate governance structures through committees that will have oversight of risks such as cybersecurity and breaches of ethical protocols.

The number of members on the audit committee, or an equivalent of the risk committee, should be increased to allow for comprehensive decision making. It is recommended to increase the number of members to three to meet the requirements of NamCode or to co-opt specialists onto the committee to render their expertise.

Risk should be a standing agenda at all board meetings as required by NamCode. This will assist organisations to be prepared and be operationally resilient through any crisis.

The culture of the board, management and employees alike is critical in maintaining an effective enterprise risk management. The board should set the tone in establishing an effective enterprise risk management function. Adequate investments should be made to enhance the risk management function, ranging from systems; people; training and communication channels, to build an effective risk management function. This has the potential to enhance the operational resilience capabilities of organisations coupled with improved adherence to the NamCode requirements, among others.

Contacts

Melanie Harrison
Director
Risk Advisory
Tel: 061 285 5003
Email: melharrison@deloitte.co.za

Kapurua Kahorongo
Manager Risk Advisory
Tel: 061 285 5019
Email: jkahorongo@deloitte.co.za

Helen Kamenye
Junior Consultant
Risk Advisory
Tel: 061 285 5025
Email: hkamenye@deloitte.co.za