

An analysis of risk management within the Department of Trade and Industry

DOI nr: <https://doi.org/10.35683/jcm192.0018>

C JOEL

University of Johannesburg, School of Public Management, Governance and Public Policy, College of Business and Economics

carmenj@uj.ac.za

S VYAS-DOORGAPERSAD*

University of Johannesburg, School of Public Management, Governance and Public Policy, College of Business and Economics

svyas-doorgapersad@uj.ac.za

* corresponding author

ABSTRACT

Risk management entails resources, planning, arranging and controlling to reduce the impact of possible risks to a manageable level. The objective of the article is to determine how the Department of Trade and Industry (DTI) implements risk management to achieve the objectives of its mandate as set out in its strategic plan, ultimately creating an ethical environment by reducing fraud. The methodology is based on a qualitative research design, using triangulation of an embedded case study with specific dimensions of unobtrusive research techniques, such as conceptual and document analysis. The Enterprise Risk Management (ERM) system is closely linked to the DTIs' risk management policy and risk management strategy objectives. The Risk Management Implementation Plan (RMIP) and the risk register, as well as the implementation of the risk management process, are instrumental in the successful risk management strategy of the DTI. The findings indicate that risk dialogue, communication, awareness, and understanding of the organisation and its risks, should be encouraged; that risk reporting practices should be strengthened, and that a better alignment between risk management and the DTIs' strategic objectives should be established.

Key phrases

Corruption; DTI; enterprise risk management; fraud; risk and risk management.

JEL Classification: Z00

1. INTRODUCTION

Risk management is a process whereby organisations methodically address the risks associated with their activities, given the goal of achieving sustained benefit within each activity, and across the portfolio of all activities. Risk management should be a continuous and developing process, which runs throughout the organisations' strategy and the implementation of that strategy (Boubala 2010:10). There are a number of obstacles that affect risk management, such as the following outlined by Williams (2017:2):

- lack of integration, where risk management is applied as an add-on rather than being integrated with other management processes, or where there is a 'silo' rather than a strategic approach at departmental level;
- a lack of systematic approach, often arising from an incorrect belief that risk management is automatically embedded in day-to-day decisions, and an absence of clear reporting to senior management and the audit committee, which tends to accompany this weakness;
- a misunderstanding of risk management, its purpose and relevance for the organisation, with some regarding it as merely a compliance exercise, accompanied by poor connectivity over risk between the top and bottom levels of the organisation, and
- an abdication of responsibility, which often arises from individuals' lack of interest in or awareness of risk, which can arise from poorly written job descriptions and a weak or absent risk management process.

In order to ensure effective risk management, the National Consumer Commission (NCC) recommends that South African public service institutions need to have the following risk management units/functions (NCC 2014:9): Financial risk: supply chain management risk, non-compliance with the Public Finance Management Act (PFMA), Treasury Regulations, safe-guarding of assets, disclosure of business interests, conflict of interest, and financial statement risk; Fraud corruption prevention and awareness: awareness programmes and fraud corruption risk registers; Functional risk: strategic risk registers, operational risk registers and process risk registers; Business continuity: preparation of a business continuity programme and Safety, health, environment occupational risk: employees' security issues, building safety and environment issues.

In the South African public service institutions, "risk management plans are not integrated into strategic planning processes. Risk management is, in the majority of instances, currently

applied as a financial matter to comply with Treasury regulations. This is also true for fraud prevention plans” (Public Service Commission (PSC) 2002:29).

This article focuses on the fraud corruption prevention awareness aspect of risk management in the Department of Trade and Industry (DTI). It provides a brief synopsis of the research methodology used for researching the various aspects which inform this article and its theoretical underpinnings. The conceptual and contextual background of the DTI is provided with a discussion on fraud, leading to the call for effective risk management in the DTI.

2. RESEARCH METHODOLOGY

The research approach in this study is qualitative in nature and will of necessity require careful description, analysis, interpretation and evaluation of the data, as well as drawing on a variety of sources for the purpose of obtaining information and relevant data. The term ‘qualitative research’ usually refers to any kind of research that builds a complex, holistic picture, and which analyses words or concepts, reports detailed information, and conducts the study in a natural setting (Creswell 1998:15). This approach is supported by Vyas-Doorgapersad (2017:145), who states that, “qualitative research (a phenomenological enquiry) seeks to understand phenomena in context-specific settings”.

Case study research, one of the most prevalent forms of social science research, is relevant when conducting research in organisations where the intent is to study systems, individuals, programmes and events. The researcher identified an embedded case study for the article. McLeod (2014:1) states that “case studies are in-depth investigations of a single person, group, event or community” or a single organisation. This article is designed around a single embedded case, where the DTI is the main unit of analysis, and the focus is its risk management processes.

The research uses extensive, multiple sources of information in data collection to provide a detailed, in-depth picture of the case and describes the context or setting for the case (Yin 2003:15). As far as analytical elements are concerned, the theoretical framework is developed in the literature analysis and incorporates the multiple variables within which the case has been embedded. A literature review in a research study accomplishes the following purposes (Creswell 1994:20-21): It shares with the reader the results that are closely related to the study being undertaken; it relates a study to the larger, ongoing dialogue in the literature about a topic, filling in gaps and extending prior studies; and it provides a framework for establishing the importance of the study, as well as a benchmark for

comparing the results with other findings. Once the findings had been identified, the literature helped the researchers to understand patterns in the data by establishing the relationships and links in the data. When drawing conclusions, the literature also helped to compare the findings of the study to those of other studies in identifying how the current study builds the knowledge base of the field by adding to, confirming, or contradicting prior findings.

There is a general scientific perception that a case study on its own cannot provide adequate scientific data for analysis and should be complemented with other qualitative research methods. Hence, to elaborate on the methodology used, conceptual analysis as an unobtrusive research method is employed to develop the analytical framework for this article. Conceptual analysis can be seen as a “system of concepts, assumptions, expectations, beliefs and theories informing the research and is generally regarded as an explanation proposed to reach a better understanding of the social reality/phenomena that is being investigated” (Ngulube, Mathipa & Gumbo 2015:47). The underlying assumptions are to assess and refine the goals; develop realistic and relevant research questions; substantiate arguments; clarify the theoretical framework and logic or reasoning used; define concepts; justify decisions, and direct data collection and analysis (Maxwell 2004:33-34). Badenhorst 2007 in Auriacombe 2011:60 explains that “conceptualising includes a reasonable, relevant researchable problem, as well as an appropriate research design and conceptual framework”. Conceptualising is a type of reasoning that begins with studying a range of specific individual cases, concepts or instances in order to extrapolate patterns from the data obtained from them, to form a conceptual category. “Conceptual analysis also relies on scholarly literature and reflections on the interpretation and interrelationships of the various related concepts and variables influencing the phenomenon” (Zongozzi & Wessels 2016:214).

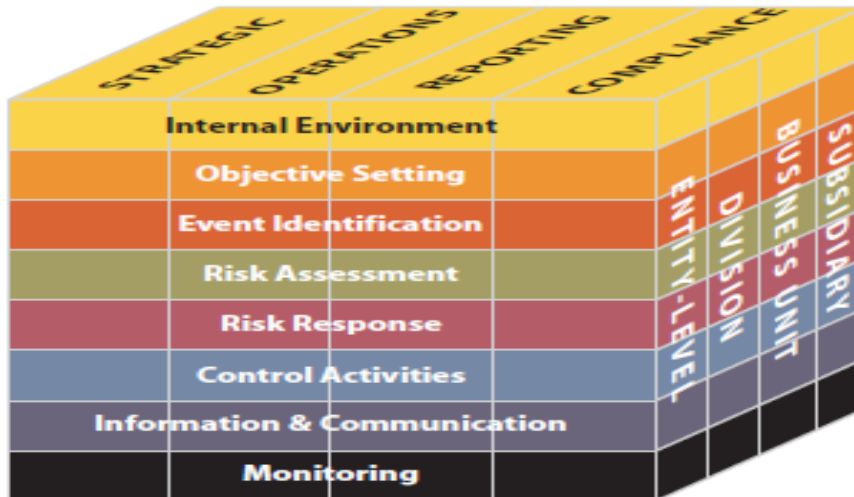
3. THEORETICAL UNDERPINNING

Enterprise Risk Management (ERM) provides a framework for risk management and is discussed as a theoretical underpinning for the article. ERM is “the strategic, enterprise-wide process of assessing, analysing and responding to the collective risks that impact an organisations’ ability to achieve its goals” (Aon 2017:1). The ERM framework (Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2004:3), is geared to achieve an organisations’ objectives, set forth in four categories such as Strategic: High-level goals, aligned with and supporting its mission; Operations: Effective and efficient use

of its resources; Reporting: Reliability of reporting and Compliance: Compliance with applicable laws and regulations.

The components and objectives of the ERM framework are portrayed in Figure 1:

Figure 1: ERM Framework



Source: COSO 2004:5

COSO (2004:3) indicates that “because objectives relating to reliability of reporting and compliance with laws and regulations are within the entities’ control, enterprise risk management can be expected to provide reasonable assurance of achieving those objectives. Achievement of strategic objectives and operations objectives is subject to external events not always within the entities’ control; accordingly, for these objectives, enterprise risk management can provide reasonable assurance that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives”.

It is nonetheless worth noting that the ERM offers various benefits to organisations to manage risk. These benefits, as listed by the Chartered Global Management Accountant (2019:2), are: “greater awareness about the risks facing the organisation and the ability to respond effectively; enhanced confidence about the achievement of strategic objectives; improved compliance with legal, regulatory and reporting requirements; and increased efficiency and effectiveness of operations”. Due to the benefits the ERM offers, risk management is introduced in the South African public sector “as a tool to assist the accounting officer to ensure that there is effective, efficient, economical and transparent use of resources. The majority of public institutions have made great strides in implementing

systems of risk management and internal controls. This improvement is attributable to various legislations, regulations and a general willingness to have good corporate governance by public sector institutions. Risk management governance structures have largely been established and policies are in place” (Shai 2015:1). By adopting an ERM Framework in risk management, public service institutions, according to Mokgatle (2013:17), could “improve the way they allocate their resources”, which “should lead to better capital efficiency and greater return on equity. In addition, ERM might induce better risk management disclosures”.

4. CONCEPTUAL CLARIFICATION

Rousseau once pointed out that the legitimacy of national public power comes from the people. The government is the executor of the sovereign. Its power comes from the peoples’ trust. When the use of public power deviates from its original track, and is abused, corruption and its concomitant problems arise (Liu 2016:172). One of the most common forms of corruption in the public sector is bribery that is “considered as a tool of developing networks and contacts for better opportunities” (Vyas-Doorgapersad 2007:285).

RSA (2004), in the public service, “corruption, is defined in the Prevention and Combatting of Corrupt Activities Act No 12 of 2004 (Naidoo 2017:76), as “fraud; financial mismanagement; gross negligence; theft; and misappropriation and abuse. Corruption is just one of several ethical and administrative transgressions which make up ‘financial misconduct’, although the term is often employed generically to describe any and all misconduct, hence it implies risk, and demands risk management measures. What is clear is that good governance makes risk management imperative”.

There is no consensus on the definition of risk. Some “of the definitions are based on probabilities, others on expected values, some on uncertainty and others on objectives. Some authors regard risk as subjective and epistemic, depending on the knowledge available, some regard it as aleatoric, due to the probabilistic character of certain parameters, while yet others give risk the ontological status independent from the person assessing it. This certainly hinders efficient risk management” (Šotić & Rajić 2015:18). The article utilises the definition provided by Cooper and Faseruk (2011:20), who defined risk as “the exposure to the chance of loss from ones’ own actions or decisions, while strategy is defined as a long-term plan of action designed to achieve a particular goal. At the government level, strategic risk may be more prevalent due to enduring periods of innovation

and finite resources. Understanding strategic risk and its impact are important to both finance and the broader management field”.

Risk management, according to Demir and Bostanci (2010:1587), “is a discipline that ensures efficient and effective utilisation of project resources, which supports decision-making based on information, and which aims to reduce uncertainties and their negative effects to a more manageable level”. The International Risk Management Standard (International Organization for Standardization - ISO 31000:2018) provides guidelines on managing risks faced by public service institutions. According to the Department of South Australia 2012:5), “the success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organisation at all levels”. Risk management therefore refers (ISO 31000:2018) collectively to the principles, framework and process for managing risks effectively.

Enterprise risk management (ERM), according to Chartered Global Management Accountant (2019:1), is the process of identifying and addressing methodically the potential events that represent risks to the achievement of strategic objectives, or to opportunities to gain competitive advantage.

5. CONTEXTUAL FRAMEWORK

5.1 Fraud in the South African public service

Risks that may occur in the area of operation of South African public service institutions include, inter alia, the following (PSC 2002:5): “social, economic, environmental (nature), system, resources (human and material), financial, fraud, loss of assets and theft, litigation, and nepotism”. The article discusses fraud in the South African public service in general and highlights some cases of fraud in the DTI, and hence calls for the effective implementation of an enterprise risk management framework to improve the current situation. The rationale behind this concern is that “fraud is an unethical practice that remains one of the biggest challenges facing the South African public sector. It is a potential threat to sustainable service delivery in many ways. For instance, fraud undermines the fight against corruption as it creates a situation where money that is meant for infrastructure and development ends up in the pockets of corrupt officials” (PSC 2007:10). Fraud, according to the PSC (2007:10), “also increases the cost of public services and slows down the much-needed service delivery to the public.

Fraud can be rooted in the behaviour and related actions of public servants, thus leading to negative material (typically financial) consequences for public service organisations". This statement is supported by Thompson (2010:95), who emphasises that when public service institutions fail "to institute and maintain an effective and correctly implemented risk management strategy it will fundamentally impede an organisations' attainment of success, as well as rendering it ethically and legally non-compliant". The current crisis is recorded in a document by the PSC (2011:38), highlighting that "while the governments' National Anti-Corruption Strategy considers risk management as a strategic consideration in the fight against corruption. Risk management is not being effectively implemented, managed or coordinated in the public service by the relevant anti-corruption units of departments where they exist".

The PSC (2011:38) further emphasised that "departments are only performing risk assessments and analysis as a function of their ongoing activities and overall management of their risks. Risk management functions are separate from anti-corruption units and the two never converge or interact, resulting in very limited extraction and analysis of fraud and corruption risks". In addition, the following additional challenges are recorded that are related to risk management practices in the public service institutions (PSC 2002:18-19): Acceptance of a risk management culture and formal commitment to the relevant processes clearly exists in some departments; Awareness levels regarding the application of risk management as a day-to-day management tool are relatively low at the middle management level of all departments; A trend is emerging whereby national control mechanisms of the past (Treasury Instructions) are re-written as provincial policy under the Public Finance Management Act and Risk management processes require adequate institutionalisation of basic good governance principles. The level of institutionalisation of the code of conduct at all levels of the administration is questionable.

The PSC is responsible for monitoring the effectiveness of risk management processes and interventions (fraud prevention measures in this scenario) in the South African public service. There is a lack of documentation available to assess the extent of fraud in the public service institutions. The latest document that is available on the PSC webpage regarding the financial misconduct in public service institutions dated back to the year 2013/2014. The article highlights the unethical financial misconduct in the public service for the year 2013/14 (PSC 2015; Thonzhe & Vyas-Doorgapersad 2017:142):

- There were 754 finalised cases of financial misconduct reported within this timeframe, of which 290 (38%) cases were reported by national departments and 464 (62%) cases were reported by provincial departments;
- The total amount of money involved in these finalised cases of financial misconduct reported by national and provincial departments was R208 268 012.35 and
- The type of financial misconduct involved and description of cases reported by departments fall into categories such as: corruption, fraud, financial mismanagement, theft, misappropriation and abuse and gross negligence. A statistical breakdown of the 754 finalised cases for the 2013/2014 financial year, shows that 209 (27.7%), the highest percentage, were categorized as '*Misappropriation and abuse*'. This was followed by '*Financial mismanagement*' with 155 (20.6%) cases; '*Theft*' with 150 (19.9%) cases and '*Corruption*' with 18 (2.4%) cases.

5.2 Fraud in the DTI

In terms of fraud and corruption, employees and the general public are encouraged to report any suspicious activities, especially concerning fraud and corruption (DTI 2013:53). This is facilitated by the fraud prevention policy, strategy, and plan, which reinforce the DTIs' commitment to "zero tolerance" of fraud and corruption. The National Anti-Corruption Hotline (0800 701 01) is part of the DTIs' "*Be silent no more*" campaign, which is supplemented by an Ethics Management Framework (Joel 2016:137). The annual reports of the DTI expose the following statistics of corruption (Mphidi 2015:7): "in 2008/2009, incidents of theft, bribery and fraud comprised 23% of misconduct cases for the financial year. In 2009/10, fraud and corruption amounted to 23% of misconduct incidents. During the 2010/11 financial year, fraud and corruption incidents amounted to 19% of the total misconduct cases, while these offences constituted 3.57% of misconduct incidents during the 2011/2012 financial year. During 2012/13 fraud and corruption totaled 5% of the total misconduct cases".

In 2015, "allegations of fraud, corruption and reckless tender appointments have surfaced in a DTI-mandated forensic report" (Cokanye 2015:2). An article published in the *The Mercury*, dated 18 September 2015 (Cokanye 2015:3), reported that "among the findings of the forensic report were an irregular tender appointment worth R65 million for bulk-earth-works and infrastructure because 10 of the 11 bidders were disqualified". The level of corruption has only increased. In 2018, it was reported that "the Hawks are struggling to solve several corruption cases reported by the DTI. This has been revealed by Trade and Industry Minister Rob Davies in a written parliamentary reply. Davies says out of 24 corruption cases reported

to the police by his department under the Prevention and Combating of Corrupt Activities Act have been closed for various reasons, including inability to locate key witnesses” (Ndenze 2018:1). These reports, according to Mphidi (2015:3), are “an indication that dishonest employees within the DTI have had the opportunity to execute fraudulent and corrupt activities and have continued to take advantage of such opportunities”. The above-mentioned DTI annual reports confirm that “such fraudulent and corrupt activities were taking place within the DTI national office” (Mbele & Mvana 2009 in Mphidi 2015:3-4).

Some examples of corruption and fraud in the DTI context are, according to Mphidi (2015:63), theft of property e.g. stationary, cash and equipment through misrepresentation; unlawful or unauthorised release of confidential information; dishonest use of intellectual property of the DTI or of its electronic systems; knowingly making or using forged or falsified documents; dishonest use of the DTIs’ computers, vehicles, telephones, credit cards, and other property or services; fabrication, falsification or plagiarism of research or scholarly work; falsifying invoices for goods or services; dishonestly using purchase or order forms for personal benefit; receiving or giving kickbacks or secret commissions to or from third parties and falsifying travel, subsistence and petty cash claims.

In order to deal with these challenges, the article utilises the ERM framework as its theoretical underpinning. It recommends that the DTI considers the ERM Framework suggested by the NCC, as it is based on the following (NCC 2017): the principles embodied in the PFMA No 1 of 1999; the Public Sector Risk Management Framework (PSRMF), published by National Treasury, Enterprise Risk Management Framework published by COSO; the International Guideline on Risk Management (ISO 31000) and the King Code on Governance Principles (King III).

6. IMPLEMENTATION OF THE DEPARTMENT OF TRADE AND INDUSTRIES’ ERM SYSTEM

The ERM framework recommends the incorporation of the following objectives: strategic, operations, reporting, and compliance. In the DTI, the following objectives are required:

Strategic: The DTIs’ Risk Management System (RMS) is composed of the risk policy, implementation plan, risk register, as well as the implementation and maintenance of the risk management process. The risk management policy clearly outlines the accountability and responsibility for risk management (DTI 2008:2). The risk management strategy is a blueprint for the manner in which the risk management policy is implemented, in conjunction

with defining how risks will be managed during their life cycle (DTI 2009:2). The implementation of the DTIs' risk management policy is facilitated by the risk management strategy. The DTI has articulated that "the risk management strategy and supporting plan will acknowledge actual and potential threats to the successful delivery on the DTI mandate and determines the activities required to minimise or eliminate them" (Joel 2016:146). Six objectives are embedded in the risk management strategy (Joel 2016:146): to "clearly identify objectives, roles, and responsibilities for managing risk; reinforce the importance of risk management as part of the everyday work of the DTI employees; improve coordination of risk management activities throughout the DTI; improve assurance to senior management and employees that the DTIs' Risk Management Unit is making every effort to reduce/eliminate risks of not achieving its objectives; and introduce a structured framework to the risk management process, through the identification, assessment, evaluation, and monitoring of risk". Formulating a risk management policy that is impractical in its implementation is deemed futile and wasteful; however, the highlighted objectives of the risk management strategy facilitate the achievement of the elements outlined in the risk management policy. The risk management strategy ensures that the theoretical aspects of risk embodied in the risk management policy will be applicable in practice. It is crucial that all these objectives are achieved to facilitate the successful implementation of the risk management policy (Joel 2016:146). The DTI aims to address all the risks within itself to ensure that no risk hinders the attainment of its objectives.

Operations: As outlined by the PSRMF, public institutions should develop an ERM system to guide risk management, by following the generic approach of the ERM. Institutions may develop ERM systems tailored for this purpose. The DTI adopted an ERM approach aligned with the PSRMF, COSO Framework, ISO 31000, and the King Reports, and developed its system through consulting and considering the relevant guidelines contained in these advisory frameworks. The process is uniquely structured, tailored to fit the objectives of the DTI and the various stages followed in the DTIs' risk management process (Joel 2016:142). Through the utilisation of its RMS, the DTI is in a position to ensure compliance and fraud prevention. The RMS consists of an enterprise-wide risk management procedure which focuses on enabling the DTI to manage risk in the most effective manner, and consists of the following tools: the risk management collaboration system (or the risk register online); the complainer calendar, and the fraud prevention matrix (DTI 2008:4). The RMIP and the risk register are also instrumental for the successful risk management strategy of the DTI. The RMIP was developed to give effect to the risk management policy and risk management

strategy. All risk management activities required for the financial year are outlined in the RMIP (DTI 2013). The RMIP ensures that all the aspects highlighted in the risk management policy and the risk management strategy is realised.

A risk register comprises one of the most important tools available to organisational risk management, and must be utilised in the most appropriate manner (Chappel 2014:114). To prevent misinformation or irrelevant results, it is crucial for the risk register to “cover the totality of the risk landscape and link directly with performance information; help support how risk managers want to think about, monitor, and manage risks and performance internally; and ensure that what matters to the company remains firmly front and centre on the Boards’ radar” (Chappel 2014:114). Risk registers can be used for various risk management processes; however, within the context of this study, only two functions are highlighted: supporting the delegation of authority, and supporting operational risk management (Chappel 2014:114). The moral ethos of the department is strengthened by an email-based ethics help desk (ethics@thedti.gov.ac). Should a staff member be required or wish to undertake remunerative activities beyond the boundaries or scope of their duties, they must obtain approval because all business ventures require disclosure. To ensure that no conflicts of interest or ethical quandaries arise, prior to the granting of approval, the Risk Compliance Chief Directorate has the responsibility of carefully scrutinising all applications (DTI 2013).

Reporting: The DTIs’ risk management structure is composed of sub-categories, each responsible for different roles and responsibilities required to ensure that the risk management process is successful. These sub-categories include the Accounting Officer (AO), who is the Director-General (DG); the EXBO; the Chief Operating Officer (COO) accountability role; Internal Auditors and Audit Committee (AC); a Risk Management Officer (RMO); other personnel involved in the management of the organisation; employees and the risk owner (RO) (Joel, 2016). The DTI national office has a risk management unit (RMU) within Corporate Governance. The DTI “has a Risk Management Policy which identifies and comes up with measures to mitigate the risks, including risks related to fraud and corruption, and advises the department” (Mphidi 2015:80) accordingly. The DTI RMU is the custodian of the Fraud Prevention Policy and Strategy, and the Policy on Protection of Whistle-blowers. These policies are some of the internal controls put in place to mitigate fraudulent and corrupt activities in the department. There is also a Risk Management Committee (RMC) to monitor risks within the DTI, and an established Audit Committee within the DTI to oversee

and assist in ensuring that the department does not misuse state funds and fall victim to fraud and corruption (Mphidi 2015:80).

Compliance: Section 38 (1) a of the Public Finance Management Act No 1 of 1999 (amended by the Public Finance Management Amendment Act No 29 of 1999), highlights that the Accounting Officer must ensure that the entity has and maintains effective, efficient and transparent systems of financial and risk management and internal controls (Republic of South Africa (RSA) 1999). The South African National Treasury Regulations (section 27.2.1) (NCC 2017), states that “the Accounting Authority must ensure that risk assessment is conducted regularly so as to identify new and emerging risks in the Organisation. The risk management strategy, which must include a fraud prevention plan, must be used to direct internal audit effort and priority as well as determining the skill required of managers and staff to improve controls while managing risks”. The Public Sector Risk Management Framework has been developed in response to the requirements of the Public Finance Management Act and Municipal Finance Management Act for Institutions to implement and maintain effective, efficient and transparent systems of risk management and control (National Treasury 2019). The King Code of Governance, Chapter 4, Principle 4.1 (King III Report, NCC 2017) requires that the governing body should govern risk and opportunity in a way that supports the organisation in defining the core purpose and to set and achieve strategic objectives.

The ERM framework demands the DTI to have provisions of ethics and ethical codes through policies and procedures. The DTI therefore has implemented a risk management policy. It is required by the DTI to incorporate strategic and operational roles in the risk management plan to obligate the policy. The DTI therefore has also implemented a RMIP where the risk register is instrumental in the successful risk management strategy of the DTI. The policy and roles need to be communicated to all employees in order to equip them with an understanding of the various types of risks and related consequences. This arrangement is further explained by Young (2006:97), who emphasises that “it is essential that risk management policies correspond with internal operations, business strategy, mission, *raison d’être*, culture, and the management philosophy of the organisation”.

In terms of fraud and corruption, South African public service institutions are obliged to follow the Protected Disclosure Act, No. 26 of 2000 (RSA 2000) that can be used as tool to protect public officials in government departments who disclose any acts of misadministration, fraud or corruption against any occupation detriment. The PSC has also published a Guide for

Public Sector Managers Promoting Public Sector Accountability Implementing the Protected Disclosure Act, to aware public servants regarding the consequences of the acts of maladministration, fraud or corruption. The DPSA has further introduced the National Anti-Corruption Hotline (NACH) that is administered by the (PSC 2004). The PSC (2006) has published a National Anti-Corruption Hotline Toolkit to inform the public and public servants of the mechanisms for reporting fraud and corruption. In addition, the public service institutions are required to have a fraud prevention policy that, in conjunction with the code of conduct, forms a part of the fraud prevention plan. The “plan is intended to serve as an additional measure to assist in the limitation of fraud and corruption risk (with a particular focus on creating awareness and promoting ethical business conduct)” (NCC 2017: 41).

In order to mitigate fraud, the DTI therefore has set out the following fraud controls in two categories (Mphidi 2015:64):

- 1) Prevention strategies, such as the ethics framework, fraud prevention strategy, fraud and ethics awareness training, fraud risk assessment, robust internal controls, and pre-employment screening;
- 2) Detection strategies, such as data analysis, management reports and reviews (including the allocation of fraud prevention responsibilities), fraud and ethics awareness training, clear reporting channels, whistle-blower protection and internal auditing.

A Fraud Prevention Policy NCC (2017:42) “sets out the stance to fraud and corruption and a prevention plan which sets out steps for the reporting/resolution of reported and identified incidents and/or allegations of fraud and corruption” in the public service institutions. These policies, plans and mechanisms form part of all South African public service institutions including DTI.

7. CONCLUDING REMARKS

This article discussed the practical application of the risk management processes in the DTI, focusing on fraud and corruption as risks in the DTI. The Companies’ Tribunal Five Year Strategic Plan 2017/18-2021/22 highlights the following operational and strategic challenges in the DTI requiring improvement (Companies Tribunal 2016:13): “lack of appropriate office space; no professional equipped hearing room; no adequate parking; external dependencies (e.g. internal audit function outsourced and Information Technology (IT) infrastructure); limited budget to optimally fill the staff establishment; limited jurisdiction of Companies Tribunal; synergy between members and management; and limited marketing and

management". Additional challenges were recorded (Lambooy & Levashova 2012:5): "many employees were leaving the DTI for a number of reasons, such as new career opportunities with other employers and drawbacks in the management style. There were issues with a lack of shared vision and leadership, which had to be changed. The key statistics regarding the vacancy rate and ultimately the performance were alarming". These observations led to a need to address the human resources aspects, and operational and strategic objectives of the DTI. These challenges have caused various forms of threats such as staff turnover and potential backlog, and employees involved in unethical practices to gain monetary benefits.

Based on the findings of the conceptual and contextual review of the information, the article suggests that the DTI:

- needs to implement mechanisms to lessen both operational and strategic risks;
- reviews all aspects of the ERM framework, as they require interconnectedness and interdependence;
- organises workshops to make employees aware of the application of the ERM framework in the institution;
- organise workshops to guide employees regarding the fraud prevention plan and code of conduct applicable in the institution;
- introduce and implement capacity-building interventions to equip employees with risk identification and detection;
- provide employees with a theoretical understanding and practical training regarding ethics, and code of conduct within the institution;
- ensure that employees attend workshops to gain an understanding of compliance mechanisms and anti-corruption measures;
- ensure that employees understand the whistle-blowing processes, preventions and measures such as toll-free telephone numbers, walk-ins, and the anti-corruption and fraud hotline toll-free number;
- Ensure that reporting levels offer guidance and assistance to subordinates regarding implementation of code of ethics in the institution;
- continuously monitor and evaluate fraud and corruption prevention measures;
- annually review and update fraud and corruption measures, given the new forms of corruption such as electronic transfer of funds, digital security and cyber fraud, to state a few;

- equip employees with electronic measures and procedures such as electronic fleet management systems, an e-procurement system, and an e-supply chain system, as well as measures to detect digitally-linked fraud;
- strengthen internal control measures for risk identification;
- control risk analysis and risk assessments annually and
- provide the PSC with compliance reports annually.

In addition, and to summarise, risk dialogue, communication, awareness, and understanding the organisation and its risks should be encouraged; risk reporting practices should be strengthened, and a better alignment between risk management and the DTIs' strategic objectives should be established.

The risk management process comprises a crucial component on which the DTI is dependent for the achievement of its ultimate goals. Throughout the entire risk management process, there are multiple, pertinent activities which require implementation, and which are significantly interconnected and mutually interdependent. The DTI has implemented several activities to administer and address corruption, immorality, or dishonest activities or issues - indicating its desire for the progressive elimination thereof - to establish an ethical and moral culture within the DTI (Joel 2016:137). It specifies that every unit in the DTI should have a risk champion responsible for assisting the risk management unit to provide reports dealing with the most current updates and progress of identified risks (DTI 2008:9). It is essential that risk champions undergo specific and appropriate risk management training to facilitate the optimal execution of their duties (DTI 2008:9). Training should incorporate both theoretical and practical training. Additionally, the Executive Board (EXBO) and senior management must provide the risk champion with the necessary support, assistance, and reinforcement (DTI 2008:10), without which risk management practices will be rendered inadequately, improvidently, or inefficiently.

The DTIs' process therefore could be considered an effective control mechanism to prevent and manage risk. The structural and functional frameworks for risk management underpin the process of risk management in the DTI by way of risk management champions, and the risk management structures that implement risk management. The ERM system is closely linked to the DTIs' risk management policy and risk management strategy objectives. The findings of this study indicate that risk dialogue, communication, awareness, and understanding of the organisation and its risks should be encouraged; risk reporting practices should be strengthened, and operational efficiency reinforced; a common risk language and lexicon should

be developed and a better alignment between risk management and the DTIs' strategic objectives established.

However, the lack of updated statistics on fraud in the South African public service limits appropriate assessments of fraud prevention plans. Future research may undertake a more critical evaluation of various risk management theories. A different methodological approach (a case methodology, for example) may be utilised to assess an appropriate risk management theory for effective implementation in a selected South African department.

REFERENCES

- AON.** 2017. Enterprise Risk Management. [Internet:https://aon.co.za/rc_enterpriseriskmanagement.aspx; downloaded on 25 February 2019.]
- AURIACOMBE CJ.** 2011. Methodology Class Lecture for Honours Students. Johannesburg: University of Johannesburg. (Unpublished document.)
- BOUBALA HGO.** 2010. Risk Management of SMMEs. Cape Peninsula University of Technology: Faculty of Business.
- CHAPPEL C.** 2014. The Executive Guide to Enterprise Risk Management. Hampshire: Palgrave MacMillan.
- CHARTERED GLOBAL MANAGEMENT ACCOUNTANT.** 2013. Enterprise Risk Management. [Internet:<https://www.cgma.org/resources/tools/essential-tools/enterprise-risk-management.html>; downloaded on 11 March 2019.]
- COKANYE R.** 2015. Fraud, Corruption, Reckless Tender Alleged by DA. *The Mercury*. (18 September 2015.)
- COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO).** 2004. Enterprise Risk Management -Integrated Framework. [<https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf>; downloaded on 11 March 2019.]
- COMPANIES TRIBUNAL.** 2016. Companies Tribunal Five Year Strategic Plan 2017/18-2021/22. Pretoria: DTI.
- COOPER T & FASERUK A.** 2011. Strategic Risk, Risk Perception and Risk Behaviour: Meta-Analysis. *Journal of Financial Management & Analysis* 24(2): 20-29.
- CRESWELL JW.** 1994. Research Design: Qualitative and Quantitative Approaches. New York: Sage Publications.
- CRESWELL JW.** 1998. Qualitative Inquiry and Research Design: Choosing among Five Traditions. Thousand Oaks, CA: Sage Publications.
- DEMIR H & BOSTANCI B.** 2010. Decision-support Analysis for Risk Management. *African Journal of Business Management* 4(8):1586-1604.
- DEPARTMENT OF SOUTH AUSTRALIA.** 2012. Risk Management Framework. [Internet:https://dhs.sa.gov.au/__data/assets/pdf_file/0008/9782/risk-management-framework.pdf; downloaded on 08 April 2019.]
- DEPARTMENT OF TRADE AND INDUSTRY (DTI).** 2008. The DTI Policy on Risk Management. Pretoria: Government Printers.
- DEPARTMENT OF TRADE AND INDUSTRY (DTI).** 2009. The DTI Risk Management Strategy and Implementation Plan. Pretoria: Government Printers.

DEPARTMENT OF TRADE AND INDUSTRY (DTI). 2013. The DTI 2013/14-2015/16 Annual Performance Plan. Pretoria: Government Printers.

DEPARTMENT OF TRADE AND INDUSTRY (DTI). 2015. Overview of the Department of Trade and Industry (DTI). [Internet:http://www.theDTI.gov.za/about_DTI.jsp; downloaded on 28 February 2015.]

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). 2018. ISO 31000:2018 Preview Risk management - Guidelines. Geneva, Switzerland: ISO.

JOEL C. 2016. Risk management best practices in the Department of Trade and Industry. Johannesburg: University of Johannesburg. (Unpublished Masters of Arts Dissertation.)

LAMBOOY T & LEVASHOVA Y. 2012. Case Study: Best practices of the Department of Trade and Industry Republic of South Africa: Human Resource and Systems Management. Pretoria: DTI.

LIU X. 2016. A Literature Review on the Definition of Corruption and Factors Affecting the Risk of Corruption. *Open Journal of Social Sciences* 4(6):1-7.

MAXWELL J. 2004. Qualitative Research Design: An Interactive Approach. 2nd ed. Thousand Oaks, CA: Sage.

MCLEOD S. 2014. Case Study Method. [Internet:<https://www.simplypsychology.org/case-study.html>; downloaded on 15 March 2019.]

MOKGATLE B. 2013. Enterprise Risk Management within Public Sector Institutions for Improving Compliance: A Case Study into a Public Sector Institution. University of Pretoria: Gordon Institute of Business Science.

MPHIDI AJ. 2015. An Analysis of the Rules and Procedures of Reporting Fraud and Corruption in the Department of Trade and Industry. Pretoria: University of South Africa. [Internet: <http://uir.unisa.ac.za/handle/10500/18818>; downloaded on 12 March 2019.]

NAIDOO V. 2017. Measuring Corruption Risk in the South African Public Service: An Institutional Analysis. *African Journal of Public Affairs* 9(6):73-87.

NATIONAL CONSUMER COMMISSION (NCC). 2014. Risk Management Strategy. [Internet:https://www.thedti.gov.za/parliament/StratPlans_APPS/NCC2017-AnnexureB.pdf; downloaded on 05 March 2019.]

NATIONAL CONSUMER COMMISSION (NCC). 2017. Enterprise Risk Management Framework. [Internet:https://www.thedti.gov.za/parliament/StratPlans_APPS/NCC2018_AnnexureA.pdf; downloaded on 13 March 2019.]

NDENZE B. 2018. Hawks Struggling to Solve Corruption Cases Reported by DTI. [Internet:<https://www.msn.com/en-za/news/other/hawks-struggling-to-solve-corruption-cases-reported-by-dti/ar-AAy6Ccj>; downloaded on 20 February 2019.]

NGULUBE P, MATHIPA ER & GUMBO MT. 2015. Theoretical and Conceptual Framework in the Social Sciences. In Mathipa ER & Gumbo MT. Eds. Addressing Research Challenges: Making Headway in Developing Researchers. Noordwyk, SA : Mosala-MASEDI Publishers & Booksellers. (pp 43-66.)

PUBLIC SERVICE COMMISSION (PSC). 2002. Integrated Risk Management In The Public Service: A Provincial Perspective. Pretoria: PSC.

PUBLIC SERVICE COMMISSION (PSC). 2004. National Anti-Corruption Hotline (NACH). PSC: Pretoria.

PUBLIC SERVICE COMMISSION (PSC). 2006. National Anti-Corruption Hotline Toolkit. Pretoria: PSC.

PUBLIC SERVICE COMMISSION (PSC). 2007. Report on the Implementation of Fraud Prevention Plans in the Public Service. Pretoria: PSC.

PUBLIC SERVICE COMMISSION (PSC). 2011. Profiling and Analysis of the Most Common Manifestations of Corruption and its Related Risks in the Public Service. Pretoria: PSC.

- PUBLIC SERVICE COMMISSION (PSC)**. 2015. Factsheet on Financial Misconduct and the Recovery of Money Lost through Financial Misconduct for the 2013/2014 Financial Year. Pretoria: PSC.
- PUBLIC FINANCE MANAGEMENT ACT (PFMA). REPUBLIC OF SOUTH AFRICA**. 1999. Public Finance Management Act of 1999 Act 1 of 1999. Pretoria: Government Printer.
- NATIONAL TREASURY (REPUBLIC OF SOUTH AFRICA)**. 2019. Risk Management Framework. Pretoria: National Treasury.
- REPUBLIC OF SOUTH AFRICA (RSA)**. 1999. Public Finance Management Act No. 1 of 1999. Pretoria: Government Printer.
- REPUBLIC OF SOUTH AFRICA (RSA)**. 2000. Protected Disclosure Act, No. 26 of 2000. Pretoria: Government Printer.
- REPUBLIC OF SOUTH AFRICA (RSA)**. 2003. Municipal Finance Management Act No. 56 of 2003. Pretoria: Government Printer.
- REPUBLIC OF SOUTH AFRICA (RSA)**. 2004. Preventing and Combating of Corrupt Activities Act No. 12 of 2004. Pretoria: Government Printer.
- SHAI J**. 2015. Landscape of Risk Management in the South African Public Sector. Pretoria: Institute of Risk Management South Africa.
- ŠOTIĆ A & RAJIĆ R**. 2015. The Review of the Definition of Risk. *Online Journal of Applied Knowledge Management* 3(3):17-26.
- THE INSTITUTE OF DIRECTORS IN SOUTHERN AFRICA**. 2009. King Report on Governance (King III). [Internet: <https://www.iodsa.co.za/page/kingIII>; downloaded on 07 April 2019.]
- THOMPSON D**. 2010. Introduction to Corporate Governance and Risk Management. Pretoria: Van Schaik Publishers.
- THONZHE N & VYAS-DOORGAPERSAD S**. 2017. The Role of Organisational Ethics Management within the South African Public Service. *International Journal of Business and Management Studies* 9(2):137-150.
- VYAS-DOORGAPERSAD S**. 2007. Corruption in the Public Sector: A Comparative Analysis. *The Journal of Public Administration* 42(5):285-299.
- VYAS-DOORGAPERSAD S**. 2017. Workplace Spirituality for Improved Productivity: A Gendered Perspective. *International Journal of Social Sciences and Humanity Studies* 9(2):143-156.
- YIN RK**. 2003. Case study research: design and methods. Thousand Oaks, California: Sage.
- YOUNG J**. 2006. Operational Risk Management: The Practical Application to a Qualitative Approach. Pretoria: Van Schaik Publishers.
- WILLIAMS J**. 2017. Rigorous Risk Management a Must-Have for Public Sector Organisations. [Internet: <https://www.accaglobal.com/us/en/member/member/accounting-business/2017/03/insights/risk-management-public-sector.html>; downloaded on 19 March 2019.]
- ZONGOZZI JN & WESSELS JS**. 2016. Variables Influencing Case Study Research Design in Public Administration: A Conceptual Framework. *Administratio Publica* 24(2):212-233.