

An Appraisal of IT Portfolio as a Risk Management Tool in the Finance Department NWPG: Factor Analytic Approach

Nehemiah Mavetera

North-West University, Mmabatho, South Africa,
Email: nehemiah.mavetera@nwu.ac.za

Ntebogang Moroke

North-West University, Mmabatho, South Africa,
Email: Ntebo.Moroke@nwu.ac.za

Terrance Selededi

North-West University, Mmabatho, South Africa,
Email: terance.sehudi@gmail.com

Doi:10.5901/mjss.2014.v5n14p113

Abstract

Information technologies have long been considered as either business drivers or enablers. In some cases however, it can be an inhibitor or risk factor. It is therefore prudent for organizations to have proper alignment of their Information Technology (IT) strategies with business strategies in order to reap the benefits of IT. More importantly, organizations must be able to assess the role played by IT as a risk factor and couple that with positive role as a risk management tool. This study investigated both the positive and negative roles of IT in the Department of Finance, North West Provincial Government (NWPG) of South Africa. This was motivated by the fact that there have been several reported cases of money laundering and misappropriation of funds in this department. This has attributed to the failure of NWPG to assess the duality of context in their IT portfolio. Quantitative measures such as the descriptive and exploratory factor analysis were used in this study. Questionnaires were distributed to employees of the department and a return rate of 72% was achieved. Factor analysis results revealed 15 items that can be grouped and explained by two factors namely, operational aspects (technical issues) and business aspects (business issues) of IT. The results also noted that the department has feasible resources to manage its risk using IT as a tool. The challenge however is the lack of neither measures nor awareness programmes to manage the risk that can be associated with IT portfolio. These measures include making employees aware of the risk control measures, reporting procedures and IT risk factors in their department.

Keywords: Risk management, factor analysis, Information Technology, North West Province

1. Introduction

Governments world over are heavily depended on IT to run their business processes. The advent of automated Information systems (IS), while regarded both as enablers and drivers of business, they however have introduced insurmountable process control and auditing problems. This is exacerbated by the fact that government institutions, having been blended around traditional manual business processes, they are also very slow in adopting and later adapting to the new technological advances that are common in the private sector. NWPG department of Finance is one such government institution that is struggling to incorporate the use of IT as a risk management tool. As a point of departure, the researchers would like to propose that firstly, there are no policies, processes and control measures that can be used to guide the use of IT as a risk management tool in the NWPG.

The researchers also note that, it is the responsibility of management of companies or organizations to see to it that policies and objectives are formulated, implemented and honored. This is to safe guard against the existing risks in the activities of the organizations and also to try and protect their stakeholders' profits. The main scope of such a project will be to manage the risk if not preventing it. Valsamakis *et al.* (2005) define risk management as a managerial function aimed at protecting the organization, its people, assets and profits against the physical and financial harm. According to

Rahul and Singh (2012), risk management is “the identification, assessment, and prioritization of risks on objectives, whether positive or negative, followed by a coordinated and economical application of resources to minimize, monitor and control the probability and impact of unfortunate events or to maximize the realization of opportunities”.

It is with this in mind that many companies, governments departments included, employ the use of risk managers. However, risk management can only be successful if the organizations have put a risk control framework in place. The framework should consist of business process, anticipated risks to each process, responsible actors for each process, control measures such as policies and guidelines to identify mitigate or eradicate the business risks. This framework becomes very important especially when most of the business processes are automated as the case in NWPG Finance department. IT, besides being used as a risk control tool, it can at times become an organizational risk itself. This needs IT to be managed. The study does not focus on IT as a risk, but as a tool that can be used to manage risk in government departments. The rest of the paper is as follows: The NWPG Finance department is discussed first. This is followed by the extant literature on IT risk management. The theoretical grounding is followed by the research methodology employed in the study. The analysis of the results and the deductions made from them are presented last.

2. Background to the NWPG Department of Finance

The Department of Finance (DoF) within the North-West Provincial Government (NWPG) in South Africa (SA) is tasked to provide good service to its customers. Coupled with some budgetary constraints as was discovered during the 2009/2010 financial year, the strategy failed because of the lack of proper management controls and poor management decisions. The 2009/2010 financial year marked the discovery by the forensic investigation team of Price Waterhouse Coopers (PwC) that the officials of the Department of Public Works, Roads and Transport have been fraudulently enriching themselves with the funds of the government. The investigations were taken over by the South African Police Service (SAPS). Some of these officials were suspended and others dismissed. Those who were not found guilty were reinstated to their jobs.

The two-month audit, conducted in 2009 into tenders issued by the North-West Department of Public Works, Roads and Transport management directorate led to the dismissal of the department’s chief financial officer and chief director. The tender scandal, described by the department’s MEC as “shocking”, saw the department spending its 2009/2010 financial budget of R525m in the first three months of the year and saw its entire three year R1.5 billion medium-term expenditure framework budget being allocated apparently without following proper protocols.

This factor was very disturbing and it left employees worried and uncertain about their future and that of the department. It was noted that managers were reluctant to take their responsibilities in relation to business operations and information technology (IT) procurement process. The study investigated the procedure used for managing risk using IT in the Department of Finance, NWPG. Also, the latent structure in the factors affecting IT as risk management tool in this department was investigated.

3. Brief Literature Review

“The average company today is a complex enterprise engulfed by rapid technological change and fierce global competition. You have to assess exposure to risk on an ever changing landscape”

Athur Levitt, Former chairperson at the US Securities & Exchange commission

From the statement above, it is noted that organizations cannot sit and rely on their founding risk management frameworks but to always continuously observe, monitor, modify and control the risk frameworks as and when the operational environment changes. As noted, in this 21st technological era, most risk are fast, and of high impact. An unsuspecting organization could easily be left out of business if their risk regulatory frameworks are not managed properly.

While Steward (2005) seems to support this view, he however noted that risk management is not meant to eliminate all risks a company may face. The point is to manage risk by choosing where to place bets and where to avoid betting altogether. This will ensure that the rewards which come due to successful risk management interventions are appreciated as well. As also noted and supported in Makhudu et al. (2012), organizational security standards should be established and a set of controls and guidelines enforced to ensure that security procedures governing the use of the organization's IT assets and resources are properly followed. Management should play a vital role in overseeing policy implementation and in ensuring the establishment of appropriate operational controls.

While there are business issues and technical issues involved in the use of IT, Stoneburner et al. (2005)

recommends that organizations should consider either technical management and operational security controls or both such controls. This should be exercised in view to maximize the effectiveness of controls for their IT systems and organization. Security controls when used appropriately, can prevent, limit or deter threat-source damage to an organization's mission.

Laudon and Laudon (2006) also noted that information systems threat may come as a result of technical, organizational and environmental factors. The threat may stem from internal users through introducing errors and accessing systems without authorization. Intruders may also access organizations' data through networks by launching denial of service (DoS) attacks or software to disrupt organizational operations. As McGaughey et al. (1994) indicated risk management is both a science and an art to identifying these threats, assessing and controlling them. Loudon (2000) also is of the opinion that hardware, software and network tools can be helpful in providing valid data which facilitate the risk management process. Furthermore, Jabbari et al. (2009) note that through the use of IT tools, integrated data to be accessed by risk management staff and risks that arise through planning and operational processes can easily be monitored. Management of these systems is also integrated (Gerber and Von Solms, 2005).

Bahli and Rivard (2005) content that while IT may cause unpredicted risks an organization can control these risks by implementing the system properly. The IT policy can also be defined according to the organization's objectives. Davis et al. (2002) recommend IT as it decreases time of processes in risk management In addition; Reed (2008) contends that stakeholder participation enhances the quality of risk management process.

There several reasons touted to support why systems require protection. These include the need to prohibit unauthorized access and malicious attack to organization's systems, to protect the software assets such as application programs, the operating system and stored information. Assmuth and Hilden (2008) advise organizations to allow different work groups to have access to general information while some items can be restricted to access by all people In conclusion, all these measures may be limited or ignored because, as Laudon et al. (2011) noted, many firms are reluctant to spend heavily on security as this is not directly related to revenue. The issues discussed in this section will be used to motivate for the theoretical framework that was used to guide this study in the next section.

4. Information Risk Management Framework

Risk management like many other business processes requires an organized way of monitoring it. This can be achieved if a framework or guiding principles are developed and implemented. KPMG (n.d.) developed a framework that considered five elements, that is, risk strategy, risk structure, risk measuring and monitoring, risk portfolio and risk optimisation. The following information risk management model, Figure 1, as adapted from the SANS Institute is one such framework. At any step of the model, IT is capable of facilitating flexibility, compatibility and integration of processes (Flanger, 2007 and Taylor, 2007).

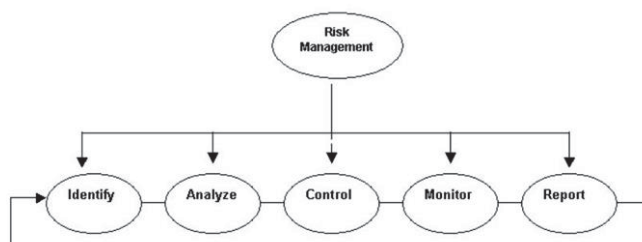


Figure 1: Adapted from the SANS Institute (2003)

The model consists of five processes that are performed in a serial fashion. This serialization is however not always the norm in reality. The constructs depicted in Figure 1 are briefly discussed below:

- Identify –this means the identification of an event that may cause information risk
- Analyze – The assessment, measurement and prioritization of threats and vulnerabilities to information for the purpose of selecting information security controls.
- Control – This is a policy, method, procedure or mechanism that addresses, identified threats and vulnerabilities to information resources.

- Monitor – The process of systematically evaluating the organization by measuring the performance of information controls in order to initiate remedial action.
- Report - The process of systematically reporting to decision makers an accurate comprehensive and coherent assessment of information risk.

These five processes are quite synonymous with those used in the KPMG_Russia framework. However, the study uses the Figure 1 framework as a lens to identify issues that must be considered by organizations when assessing IT risk control factors.

5. Objectives of the Study

As motivated earlier, the aim of the study is to investigate IT as a Risk Management tool in the Department of Finance (DoF), North West Provincial Government (NWPG) in South Africa. Several objectives were identified and these were directly addressed using the empirical data that was collected in the IT sub-directorate of the Department of Finance. These objectives are listed below as:

- (a) To determine the skills level of personnel responsible for operating the financial systems
- (b) To determine the state of IT resources in the department
- (c) To investigate the measures in place to ensure control and reporting of activities and risks in the department
- (d) To determine the measures employed by the Department of Finance to reduce the IT risk
- (e) To determine the security controls available in the Department of Finance
- (f) To explore the factors predicting IT as a risk management tool within the Department of Finance NWPG

Other objectives that were silently discussed and addressed through literature study are:

- To determine the success of IT in risk management tool
- To determine the intervention strategies available to IT management in case of emergency

The next section discusses the research methodology that was used in this study.

6. Research Methodology and Design

This study used a quantitative survey research approach. Descriptive statistics were used to analyse the data collected. The intention for using descriptive statistics was to gather evidence from respondents concerning the degree to which they agree or disagree to the four constructs on the questionnaire.

6.1 Questionnaire

The instrument used for collecting data was a questionnaire. Set of construct items were developed and aggregated into a five point Likert scale with 1 representing Strongly Disagree, 2 Disagree, 3 Neutral, 4 Agree and 5 Strongly Agree. The choice of a five-point odd number scale was informed by the fact that some respondents may completely fail to make a decision. This then will be reflected with the neutral response. Five sections constitute the questionnaire, with Section A addressing the demographical data of the respondents and the rest of the four sections relating to the study objectives. The questionnaire was self-administered to avoid bias and some questions not being answered.

6.2 Sample

The targeted population for this study was employees of NWPG IT sub-directorate in Finance Department. The department has a total of 66 employees including those who are placed in the regions. Since the population size was very small, it was considered prudent to sample the whole population. This implies that N (population) and n (sample) return rate of 72% was achieved. The sample comprised of Management, Networking, Data Technology, Security and Help Desk staff.

7. Empirical Analysis and Results

The Statistical Package for Social Sciences (SPSS) version 21 was used to analyse the data. The results of this analysis are presented in Tables 1 through to 4.

7.1 The Research Study Results

Table 1: Demographic data analysis

Variable	Category	Responses	
		n	%
Gender	Female	30	62.5
	Male	18	37.5
Race	African	42	87.5
	Coloured	2	4.2
	Indian	1	2.1
	White	3	6.3
Job function	Director	1	2.1
	Manager	2	4.2
	Supervisor	7	14.6
	Technical	23	47.9
	Other	15	31.3
Qualification	Post Graduate	5	10.4
	Bachelor Degree	8	16.7
	National Diploma	13	27.1
	Matric	21	43.8
Work experience	1-5	10	20.8
	6-10	17	35.4
	11-15	10	20.8
	16 -above	11	22.9

From a survey of 48 employees in the IT section, Department of Finance in the NWPG, it is noted that females are the majority (62.5%) as opposed to 37.5% of males. For a department located in the North West Province of South Africa, it is not surprising to notice Black employees being in majority (87.5%) than people of other race groups. From the four sub-directorates in the department, 47.9% comprise of technical workers and 14.6% supervisors, with 31.3% constituting people employed in other positions. The majority of employees in this department have been in employment for more than 6 years and most of them have matric and diplomas being their highest qualifications. The statistics above indicate that if IT as a risk management tool is to be assessed, the staff in the IT section is capable of giving a reliable assessment since majority of them have worked for more than six years in the department.

7.2 Revisiting the Research Objectives

To determine the state of IT resources in the department

Table 2: State of IT resources

Construct	Strongly Disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
All applications and software used in IT have current licenses	6 (12.5)	10 (20.8)	14 (29.2)	14 (29.2)	4 (8.3)
All production servers, applications and supporting software are physically located in the data centre	5 (10.4)	7 (14.6)	11 (22.9)	21 (43.8)	4 (8.3)

37.5 % compared to 33.3 % indicated that the application software running in the department is licensed. From a risk perspective, licensed software applications can always be upgraded and the security is continuously improved. One can infer that the use of unlicensed software can be a source of IT risk to the business. The following section discusses the next objective addressed by the study.

- To investigate the measures in place to ensure control and reporting of activities and risks in the department

Table 3: Measures of risk control

Construct	Strongly Disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
I know what to do, whom to contact in case of fire, accident, and inappropriate physical access	3 (6.3)	11 (22.9)	9 (18.8)	18 (37.5)	7 (14.6)
There is a process to communicate new policies and procedures to the staff and training is provided if necessary	12 (25)	11 (22.9)	14 (29.2)	10 (20.8)	1 (2.1)
There are legal, regulatory, and Policy requirement relative to the delivery of automated services in IT	9 (18.8)	6 (12.5)	18 (37.5)	14 (29.2)	1 (2.1)
I can demonstrate compliance with applicable standards, Legal and regulatory requirements implemented in IT	13 (27.1)	6 (12.5)	17 (35.4)	12 (25.0)	0 (0.0)
There is IT planning process that is designed by management that adequately includes operational resources to support the automated line business.	11 (22.9)	9 (18.8)	14 (29.2)	14 (29.2)	0 (0.0)
Total %	Do not concur (37.94%)		Not sure (30.02%)	Concur (32.1%)	

Makhudu *et al.* (2012) highlight the importance of IT security policies in an organization. However, they noted with regret that most employees are not aware of these policies. In light of this finding, it is noted in Table 3 that NWPG IT section, Department of Finance staff might not be able to use IT as a risk management tool. This supported by the fact that 47.9% versus 22.9 % disagree that there are processes in place to inform the on IT policies. In addition, there is also no training in place to raise awareness of these policies.

However, an equal number of staff (31.3%) do agree and disagree that IT regulatory processes are available. It must be mentioned that the 37.5% of neutral respondents can add to the fact that these policies are not promulgated. This supports the lack of awareness training as indicated earlier.

To determine the measures employed by the Department of Finance to reduce IT risk

Table 4: Measures to reduce risk

Construct	Strongly Disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
Risk, including IT risks, are communicated by management in terms of their impact on business	13 (27.1)	5 (10.4)	13 (27.1)	16(33.3)	1 (2.1)
There is a business process approach to risk management technology	15 (31.3)	5 (10.4)	16 (33.3)	12 (25.0)	0 (0.0)
There is a procedure in the department for checking professionals' credentials, background and references in the department	19 (39.6)	6 (12.5)	8 (16.7)	15 (31.3)	0 (0.0)
There is operational support for risk management and accountable ownership of risk by IT management in the department.	17 (35.4)	1 (2.1)	16 (33.3)	14 (29.2)	0 (0.0)
Total %	Do not concur (42.2%)		Not sure (27.6%)	Concur (30.23%)	

On the four construct used to judge the measures in place to reduce risk, the majority of respondents (69.8 % (if we include the neutral as well) do not feel that there are sufficient measures to reduce risk in the NWPG. Reflecting on this finding, it is noted that, IT as a risk management tool is only an enabler and not a driver. If there are no sufficient business side policies, processes and procedures that focus on mitigating the general business risk, then IT does not find its role as a risk management tool as well.

To determine the security controls available in the Department of Finance

Table 5: Security controls in place

Construct	Strongly Disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
There is a backup strategies developed for continuity of automated services should the department have an IT system failure.	9 (18.8)	6 (12.5)	7 (14.6)	15 (31.3)	11 (22.9)
If an IT system failure result in a newsworthy event, wide spread will be communicated to the users via global e-mail by IT personnel	7 (14.6)	2 (4.2)	3 (6.3)	20 (41.7)	16 (33.3)
There is a secured infrastructure (password, PC, Firewall, Network policies, Procedures and hardware, Software) that protect the information asserts (data integrity, confidentiality, availability) been developed, implemented, and communicated.	6 (12.5)	5 (10.4)	6 (12.5)	22(45.8)	9 (18.8)
IT management staff are considered directly responsible and accountable if elements within the automated system failed.	10 (20.8)	6 (12.5)	7 (14.6)	14 (29.2)	11 (22.9)
Total %	Do not concur (26.58%)		Not sure (12%)	Concur (61.48%)	

The four constructs used to measure the presence of security controls in the NWPG provided an indication that indeed there are IT controls in the place in the department. However the success of IT controls or their failure is considered to be the responsibility of IT personnel in the department. Having discussed the IT risk management indicators separately, the study used factor analysis technique to group these findings and explore the factors predicting IT as a risk management tool within the Department of Finance NWPG.

7.3 A Brief on Factor Analysis

This technique is mainly used as a dimension reduction method in this study. For this reason, it is used to investigate the factors used to predict IT risk management tool in the DoF NWPG. Multi-item constructs were used in this study to capture information about different variables used in IT risk management. Prior to performing factor analysis, the suitability of data for this method is assessed through the inspection of the correlation matrix. This matrix should have as fairly high correlations between the variables being investigated as is possible. Norusis (1994) suggests that more than half the coefficients in the correlation matrix should be greater than 0.3. This gives an indication that the correlation matrix has large correlation with at least one of the other variables in the set. As Churchill (1995) pointed out, a pattern of low correlations throughout the matrix indicates a heterogeneous set of items suggesting the matrix may be inappropriate for factoring.

Additionally, to ensure the adequacy of the sample used in this study, Kaiser (1974) suggested measures in the ranges: 1 to 0.9 be characterized as marvelous, 0.8 and 0.89 as meritorious, 0.7 to 0.79 as middling, 0.6 to 0.69 as mediocre, 0.5 to 0.59 as miserable and 0 to 0.49 as unacceptable. The Kaiser-Meyer-Olkin (KMO) measure is used in conjunction with the Bartlett's test of sphericity. The null hypothesis for the latter is that the inter-correlation matrix comes from a population in which the variables are non-collinear, i.e. an identity matrix and the non-zero correlations in the sample matrix. Churchill (1995) suggests that for the analysis to be satisfactory, the hypothesis be rejected at least at the 5% level of significance. This is achieved if the observed probability does not exceed the level of significance ($\alpha < 0.05$).

Another way of telling whether or not the instrument collected data measuring the same construct is by using the Cronbach's alpha. This is a commonly used measure of internal consistency of the instrument. Owing to the multiplicity of the variables measuring the factors, the Cronbach's alpha is considered most suitable in this study since it has the most utility of multi-item scales at the interval level of measurement (Cooper and Emory 1995). A commonly accepted rule of thumb for describing internal consistency using Cronbach's according to Kline (1999) and Cronbach and Shavelson (2004) is as follows: $\alpha \geq 0.9$ is excellent, $0.8 \leq \alpha < 0.9$ is good, $0.7 \leq \alpha < 0.8$ is acceptable, $0.6 \leq \alpha < 0.7$ is questionable, $0.5 \leq \alpha < 0.6$ is poor and $\alpha < 0.5$ is unacceptable.

Prior to factor extraction, the researcher needs to determine the number of factors. Fabrigar and Wegener (2012) recommend that researchers must try to balance parsimony and plausibility when it comes to selecting the number of factors to include in a model. Parsimony refers to a model with relatively few factors and plausibility entails that there should be enough factors to adequately account for correlations among measured variables. Kaiser's criterion is considered in this study to help choose number of factors to work with. This measure relies on the eigenvalues. The eigenvalue of a factor represents the amount of variance of the variables accounted for by that factor. The lower the

eigenvalue, the lesser that factor contributes to the explanation of variances in the variables (Norris and Lecavalier, 2009). The thumb rule for Kaiser’s (1974) criterion is that the number of factors (m) to be retained must be equal to the number of eigenvalues greater than or equal to 1 ($\Lambda \geq 1$). Rencher (2002) also notes that “this is a popular criterion of long standing and is a default in many software packages”. Nyamugure *et al.* (2011) support this criterion as it eliminates values of the eigenvalues less than 1. The rationale for using this rule is that, each factor should account for at least the variance of a single variable (Darlington, 2004).

Once the statistics discussed above have been looked at, factors are extracted using Principal Component Analysis (PCA) and rotated using the varimax rotation for ease of interpretation. This type constrains factors to be correlated. It has an advantage of revealing simplicity and clarity and a disadvantage of ignoring the possibility of correlations among the constructs. This measure is more likely to produce solutions with simple structure (Fabrigar *et al.* (1999). According to Guadagnoli and Velicer (1988), if factors possess four or more variables with reasonable number of loadings exceeding 0.6, the pattern may be interpreted whatever the sample size used. Table 6 presents these factor analysis results.

Table 6: Factor analysis correlation matrix

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1.000	.384	.468	.270	.441	.525	.352	.595	.509	.559	.508	.452	.508	.365	.407
2	.384	1.000	.483	.403	.501	.489	.480	.515	.590	.532	.476	.467	.579	.434	.555
3	.468	.483	1.000	.526	.529	.544	.372	.542	.451	.484	.493	.554	.509	.448	.429
4	.270	.403	.526	1.000	.583	.589	.648	.415	.317	.408	.501	.471	.422	.429	.457
5	.441	.501	.529	.583	1.000	.743	.672	.663	.644	.627	.681	.637	.646	.442	.615
6	.525	.489	.544	.589	.743	1.000	.749	.676	.696	.637	.671	.677	.571	.599	.700
7	.352	.480	.372	.648	.672	.749	1.000	.566	.518	.516	.590	.589	.455	.542	.590
8	.595	.515	.542	.415	.663	.676	.566	1.000	.785	.753	.675	.644	.639	.510	.668
9	.509	.590	.451	.317	.644	.696	.518	.785	1.000	.747	.664	.585	.610	.514	.671
10	.559	.532	.484	.408	.627	.637	.516	.753	.747	1.000	.730	.579	.537	.436	.535
11	.508	.476	.493	.501	.681	.671	.590	.675	.664	.730	1.000	.678	.583	.512	.592
12	.452	.467	.554	.471	.637	.677	.589	.644	.585	.579	.678	1.000	.715	.682	.656
13	.508	.579	.509	.422	.646	.571	.455	.639	.610	.537	.583	.715	1.000	.664	.759
14	.365	.434	.448	.429	.442	.599	.542	.510	.514	.436	.512	.682	.664	1.000	.774
15	.407	.555	.429	.457	.615	.700	.590	.668	.671	.535	.592	.656	.759	.774	1.000

A close inspection of the correlation matrix in Table 6 reveals the presence of many coefficients greater than 0.3. This is consistent with the suggestion by Norusis (1994) about the factorability of the matrix and is also an indication that factor analysis can be applied in the current data.

Table 7: KMO and Bartlett’s Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.	0.914
Approx. Chi-Square	520.315
Bartlett’s Test of Sphericity	df
	105
	Sig.
	0.000

The KMO is marvelous (0.914) as revealed on Table 7 and satisfies the suggestion by Kaiser (1974). This implies that the sample used in this study is adequate and allows factor analyses to be carried out. The KMO values for individual items are also marvelous emphasizing that all these items can all be used in the factor analysis method. The Bartlett’s test of sphericity reached statistical significance, supporting the conclusion drawn from interpreting the KMO. These findings verify the sampling adequacy as recommended by Fidell (2009) and Churchill (1995).

Table 8: Reliability measures

Cronbach’s Alpha	Cronbach’s Alpha Based on Standardized Items	Number of Items
0.950	0.950	15

Cronbach’s alpha has been computed for the 15 items in the instrument. As displayed in the table, overall alpha is 0.950

which is excellent as described by Kline (1999) and Cronbach and Shavelson (2004). This is an indication of strong internal consistency and reliability among the 15 items.

Table 9: Kaiser Criterion

Component	Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings
	Total	% of Variance	Cumulative %	Total
1	8.889	59.260	59.260	7.732
2	1.062	7.082	66.342	6.881

The results reveal two Eigen values greater than one, suggesting that two factors are extracted from the fifteen items. This is consistent with the proposition by Nyamugure *et al.* (2011) and is also in accordance with the rule of thumb. The combination of these components explains 66.34% of the variance. The factor loadings after rotation are shown on Table 10 below.

Table 10: Rotated component matrix

Item	Component	
	1	2
1. If an IT system failure results in a newsworthy event, it will be communicated to the users via global e-mail	0.818	
2. There is secured infrastructure that protects information asserts that have been developed, implemented, and communicated	0.804	
3. There is a backup strategy developed for continuity of automated services should the department have an IT system failure	0.804	
4. All applications and software used in IT have current licenses	0.758	
5. IT management staff are considered directly responsible and accountable, if elements within the automated system fail	0.651	
6. There is a business process approach to risk management technology	0.610	
7. All production servers, applications and supporting software are physically in the data centre	0.543	
8. There is a process to communicate new policies and procedures to the staff and training is provided		0.840
9. IT planning process is designed by management		0.799
10. I can demonstrate compliance with applicable standards, legal and regulatory requirements implemented in IT		0.691
11. There is a procedure in the department for checking professionals' credentials, background and references in the department		0.667
12. There is operational support for risk management and accountable ownership of risk by IT management in the department		0.643
13. There are legal, regulatory, and Policy requirement relative to the delivery of automated services in IT		0.641
14. Risk, including IT risks, are communicated by management in terms of their impact on business		0.631
15. I know what to do, whom to contact in case of fire, accident, and appropriate physical access		0.510

In Table 10, component 1 has seven items loading on it and component 2 is explained by eight items. As Guadagnoli and Velicer (1988) suggested, the two patterns are interpreted because they contain more than four items with most of the loadings above 0.6. Component 1 can be regarded as explaining the operational aspects (technical issues) of IT while Component 2 explains largely the business side (business issues) of IT.

As noted earlier, the component 1 aspects seem to be well understood by the respondents. Since they are of a technical nature, these support the fact that respondents are IT sectional staff. However, Component 2 items which are of a business nature are poorly understood by the respondents. It can also be inferred that the factoring outcome indicates a lack of alignment between the IT and business sides in the organization. Also, this is a clear indication that IT staff is not usually well informed of the business side. This makes the issue of using IT as a risk management tool even more difficult for the IT section.

8. Conclusion and Recommendations

The aim of the study was to investigate the use of IT as a risk management tool in the department. The descriptive

statistics was used to address the first four objectives of the study and factor analysis was employed to answer the last objective. The study noted that there is confusion about the success of IT as risk management tool in the department.

Based on the findings of this study, the authors recommend that the management of the Department of Finance implement policies regarding the measures used to control risk, procedures for reporting of activities and risks in the department or to create awareness and provide training to employees about these processes. The application of factor analysis is also recommended to study related factors in all the organizations that use IT as risk management tool.

References

- Assmuth, T. & Hildén, M. (2008). The significance of information frameworks in integrated risk assessment and management. *Environmental Science Pollution*, 11, 71- 86.
- Bahli, B. & Rivard, S. (2005). Validating Measures of Information Technology Outsourcing Risks Factors. *Omega*, 33(2), 175-187
- Churchill, G.A. (1995). *Marketing Research: Methodological Foundations*. Illinois, Dryden Press.
- Cooper, D.R. & Emory, C.W. (1995). *Research Methods Homewood*, IL. Richard D. Irwin Inc.
- Cronbach, L.J., & Shavelson, R.J. (2004). My Current Thought on Coefficient Alpha and Successor Procedures, *Educational and Psychological Measure*, 64(3), 391-418.
- Darlington, R.B. (2004). Factor Analysis. Retrieved from <http://comp9.psych.cornell.edu/Darlington/factor.htm>.
- Davis, P. Dibrell, C. D. & Janz B (2002). The impact of time on the strategy performance relationship: Implications for managers. *Industrial Marketing Management*, 31(4), 339-347.
- Fabrigar, LR, Wegener, D.T., MacCallum, R.C. & Strahan, E.J. (1999). Evaluating the use of Exploratory Factor Analysis in Psychological Research. *Psychological Methods*, 4(3), 272-299.
- Fabrigar, L.R. & Wegener, D.T. (2012). *Understanding Statistics: Exploratory Factor Analysis*. Oxford University Press, New York, NY.
- Fidell, A. (2009). *Discovering statistics with SPSS*. London. Sage.
- Flanger, R. (2007). Management Risk for an Uncertain Future. The University of Reading. [Online], Available:<http://www.bre.polyu.edu>.
- Gerber, M. & Von Solms, R. (2005) Management of Risk in the Information Age. *Computers and security*, 24(1), 16-30.
- Guadagnoli, E. & Velicer, W.F. (1988). Relation of Sample Size to the Stability of Component Patterns. *Psychological Bulletin*, 103, 265-275.
- Jabbari, G M, Asilian, H, Mortasavi, S.B, Zarringhalam, M A, Hajizadeh, E, & Khavanin, A. (2009). Comprehensive Risk Assessment and Management of Petrochemical Feed and Product Transportation Pipelines. *Journal of Loss Prevention in the Process Industries*, 22(4), 533-539.
- Kaiser, H.F. (1974). An index of Factorial Simplicity. *Psychometrika*, 39, 34-36.
- Kline, P. (1999). *The Handbook of Psychological testing* (2nd Ed.). London: Routledge.
- KPMG_Russia(n.d), Identifying and monitoring risks. [Available] Online:https://www.kpmg.com/RU/en/topics/Audit-Committee-Institute/Publications/Documents/toolkit/App1_Identifying_and_assessing_risks_eng.pdf. Accessed: 22 April 2014.
- Laudon, K.C. & Laudon, J.P. (2006). *Management Information Systems, Managing the Digital Firm*, 9th Ed, Prentice-Hall of India Private Limited, New Delhi, India.
- Laudon, K.C. & Laudon, J.P. (2011). *Management Information Systems: Managing the Digital Firm* (12th Ed). Pearson Education Limited.
- Makhudu, AB., Mavetera, N. & Mavetera, C.G. (2012). *Investigating Information System Security Policy and Awareness Training Programs in South African Organizations*. In Innovation Growth, Entrepreneurship, and Economic Development. Proceedings of 19th International Business Management Association (IBIMA) conference, Barcelona, Spain, Nov 12-13, 2012. ISBN: 978-0-9821489-8-3.
- McGaughey, R.A., Snyder, C.H. & Carr, H. (1994). Implementing Information Technology for competitive advantage. *Risk Management issues*, 273-280.
- Norris, M. & Lecavalier, L. (2009). Evaluating the use of Exploratory Factor Analysis in Developmental Disability: Psychological Research. *Journal of Autism and Developmental Disorders*, 40(1), 8-20.
- Norusis, M.J. (1994). *SPSS Professional Statistics User's Manual*. SPSS Inc. Chicago.
- Nyamugure, P., Lesaoana, M. & Monyai, S. (2011). Application of Factor Analysis on the 2009 General Household Survey of South Africa. *ICASTOR Journal of Mathematical Sciences*, 5(1), 133-150
- Rahul, S. & Singh, G. (2012). Risk Management in Information Technology System. *VSRD-International Journal of Computer Science and Information Technology*, 2 (3), 190-209.
- Reed, M. (2008). Stakeholder participation for environmental management, PP 2420- 2421.
- Rencher, A.C. (2002). *Methods of Multivariate Analysis*. Wiley-Interscience, (2nd ed.) ISBN 0-471-41889-7.
- SANS Institute (2003). SANS Security Essentials: *Risk Management and Auditing*, 1(3) 865.
- Steward, T.A. Managing risk in the 21st Century. Fortune Magazine, 7 February 2000.
- Stoneburner, G., Goguen, & Feringa, A. (2005). Risk Management Guide for Information Technology Systems. *Computers & Security*, 24(2), 147-159
- Taylor, N. (2007). A note on the importance of overnight information in risk management models. *Journal of Banking and Finance*, 161-180.
- Valsamakis, A.C., Vivian, R.W. & Du Toit, G.S. (2005). *Risk management: managing enterprise risks*. 3rd ed. Sandton: Butterworth/Heinemann Higher South Africa.