The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 12 || Pages || PP -54-60|| 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Challenges to the Implementation of Information Technology Risk Management and Compliance in Zimbabwean State Universities

Paul Mupfiga, Theo Tsokota and Patrick Mamboko
Midlands State University, Zimbabwe

----------ABSTRACT----------
The paper was purposed at finding the challenges to the implementation of IT risk management and compliance in State universities in Zimbabwe. The existing risk management and compliance processes and frameworks at these universities were assessed. The participants of this research were university councilors, the principal officers, ITS directors and university employees. The research revealed that the culture of risk management is being enforced at universities top levels but there is no communication and training on the launch and implementation of the current risk management frameworks in use at lower levels. It also found out that the IT policies in all the universities were still being drafted and were not yet implemented. The research recommended the implementation and completion of drafting of the IT policies, communication of the IT policies and promotion of the use of the risk frameworks in all university departments, use of flat communication and decision making structures and recommended enforcement of the culture of risk management at low level so as to overcome the challenges to the implementation of IT risk management and compliance.

Keywords: *IT governance, IT risk management, risk framework, IT policy, compliance and information technology*

Date of Submission: 01 June 2015 Date of Accepted: 15 December 2015

I. INTRODUCTION

The study purposed to find out how state universities have implemented IT risk management and compliance in order to achieve good IT governance practises. The goal of this study was to analyse the extent to which IT risk management and compliance has been practised in Zimbabwean state universities. According to Chitanana, et al (2008), state universities in Zimbabwe have invested a lot of financial and human resources in information technology since the year 2000 and most of them have computerised their administrative functions and processes, such as, learning methods, student registration, student records and employee records.

A university's electronic information assets are amongst its most important and crucial assets. These electronic information assets are constantly exposed to threats during storage, processing and transmission, that is, unauthorized access, unauthorized changes and loss, which, if they materialize, can result in risks that can damage the electronic information assets and have serious consequences for the university. According to Von Solms (2006), many universities have started moving towards leveraging ICT systems as delivery platforms in educational, teaching and assessment programs. Such institutions run a very big risk by tightly integrating information and communications technology (ICT) as a delivery medium in educational, teaching and assessment programmes. From the technological developments at universities, it was noted that there is a huge reliance and dependency on IT services due the size of the investments that has been made over years. The universities depend on IT products and services to a very large extent, thus their level of exposure to IT risks is great and it calls for IT risk governance and management. Failure of these IT systems and services will affect service delivery by the universities, the academic standard of the institutions may deteriorate significantly and the image of the institutions will consequently suffer, that is, it will tarnish their reputation. The management of risks is a cornerstone of IT governance, ensuring that the strategic objectives of the business are not jeopardized by IT failures. Risks associated with technology issues are increasingly evident on board agendas, as the impact on the business of an IT failure can have devastating consequences (ITGL, 2005). Tarantino et al (2008) state that IT Risk management, and compliance covers an organization's approach across areas of governance, risk management and compliance (GRC). Being closely related concerns, governance, risk and compliance activities are increasingly being integrated and aligned to some extent in order to avoid conflicts, wasteful overlaps and gaps.

This study is essential in that it provides the basis upon which universities in Zimbabwe can successfully implement IT risk management policies. This in turn adds on to their competitive advantage. The identification of gaps in the existing systems is panacea as it provides an insight into areas that immediately need attention.

II. RESEARCH QUESTIONS

The study sought to answer the following research questions;

- Which challenges are being faced in implementing IT risk management and compliance?
- How the universities are governing their IT risks?
- How the IT risk management culture is being inculcated in state universities?

III. WHAT IS IT RISK MANAGEMENT

IT risk management has generated many different definitions. The King III Report on Governance for South Africa of 2010, defines IT risk management as addressing the safeguarding of IT assets, ensuring adequate disaster recovery and ensuring the continuity of IT operations and it should be the responsibility of the board of directors. The National Computing Centre's IT governance strategy guide of 2005, states that, the management of risks is a cornerstone of IT Governance, ensuring that the strategic objectives of the business are not jeopardised by IT failures. IT related risks are increasingly a Board level issue as the impact on the business of an IT failure, be it an operational crash, security breach or a failed project, can have devastating consequences.

I S A C A(2009) and ENISA(2006) defined IT risk management as the application of risk management to Information technology context in order to manage IT risk, that is, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an orgnisation. IT risk management can be considered a component of a wider enterprise risk management system. The CISA Review Manual 2006 provides the following definition of risk management, it is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization. There are two things in this definition that may need some clarification.

According to the ISACA risk IT framework of 2009, IT risk management provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues. It enables enterprises to understand and manage all significant IT risk types, thus, providing tangible business benefits, hence allowing the enterprise to make appropriate risk-aware decisions.

this research adopts, the King III Report on Governance for South Africa of 2010's definition because it covers key areas of IT risk management which are safeguarding of IT assets, ensuring adequate disaster recovery and ensuring the continuity of IT operations and it should be the responsibility of the board of directors. Furthermore the King III Report on Governance for South Africa of 2010's definition delimits the scope of this research thus making it focused.

IV. RESEARCH METHODOLOGY

The research methodology used was a triangulation which involves the use of three different methods to collect data from a given population. Structured questionnaires, interviews and document review were used. The questionnaires were designed to obtain information concerning the challenges to the implementation of IT risk management and governance. Interviews with IT directors were contacted to clarify issues raised in the questionnaire. The researchers randomly selected five universities from five Zimbabwean provinces so as to attain a national perspective. The number of case study institutions selected for this research satisfies the recommendations of Travers (2001) which recommends a sample of between 4 and 10 cases for in-depth qualitative case studies. A multiple case study approach was used to carry out the study. As suggested by Saunders, Lewis, and Thornhill (2009) the case research method is useful for addressing the "how", "why" questions, that is, in the exploratory and explanatory research. This is particularly useful for a study on IT Risk Management in the context of institutions of higher education in Zimbabwe very little is known about IT Risk Management. A case research strategy provides a rich insight in this context.

Data was gathered using questionnaires and a total of 345 questionnaires were distributed to Councillors, Principal Officers and other University employees. From the 345 questionnaires which were sent to the target population, only 300 were returned. The reasons for this response was that some respondents said there were too

busy to give time to our questionnaire, some were not sure about the real intentions of the researcher as they felt that the questionnaire was too inquisitive and the issue of risk management is viewed as sensitive. To overcome some of these issues the researcher had to visit some councillors at their respective work places for face to face meetings and to prove and explain that the research was only for academic purposes and for the purposes of progress the researcher had to track local university council members, who are senate members appointed by the Vice-Chancellors into the university councils persuading and explaining the purpose of the study and answering their queries. The researcher also distributed the questionnaire to the members of the universities' risk committees so that the research becomes a true reflection of the challenges to the implementation of IT risk management and compliance at Universities.

The interviews gathered data on IT Risk Management practices these institutions and also clarified particular issues which were raised from the questionnaires. The interviews were recorded and later transcribed and analysed using discourse analysis.

V. PREVALENT IT RISKS

The researcher obtained the IT risks prevalent through interviews with the ITS directors. The directors revealed that the universities have managed to contain IT risks to date and the following IT Risks which constitute possible threats to the universities were noted, equipment failure (hardware Failure), Incompatibility, that is, the ability of the current technology in use at the university may fail to work in conjunction with the latest technologies. Power failures, fire, tricky/Cunning Suppliers or Service Providers, that is, IT service delivery may be affected if a supplier or service provider decides to default on their delivery obligations hence the image of the university may suffer. Floods, computer viruses, software Failure, computer accidents, that is, a serious computer accident to a member of staff or a group through computer equipment use or failure or could have a serious adverse effect on the reputation and image of the university. Ballooning number of students, unauthorised access, theft, scalability/flexibility, that is the ability to easily expand or increase the university's computer networks or equipment, that is, it is fixed, rigid or flexible. However the directors revealed that the list is not an exhaustive list of all conceivable IT risks as the process of risk management is on-going and continuous thus it is subject to change at anytime. The universities have put various controls in place in order to mitigate these IT risks. The controls include the use of administrative controls which includes polices and frameworks for guidance. For instance all the universities are currently developing an IT risk policies through their computer committees and ICT risks sub-committee. The use of input controls which govern system access or entry through the promotion of the use of passwords and firewalls. Storage controls which involves the use of data back-up and encryption, the use of physical protection of computer assets and disaster recovery strategies such as the insurance of computer assets and copyrights on in-house developed software.

VI. RISK MANAGEMENT STRATEGY IN THE UNIVERSITIES

As regards to the presence of a risk strategy in the universities 77% of the respondents indicated that they had knowledge of the presence of one. Sixty-nine per cent (69%) indicated that there is someone responsible for ensuring that the universities has risk management procedures in place that cover the likely risks such as IT Risks, Occupational Health and Safety, environmental compliance, fraud and risk to the reputation of the university. A considerable number of respondents, (34%), indicated that the person responsible for ensuring that the university has risk management procedures in place that cover the likely risks such as IT Risks, Occupational Health and Safety, environmental compliance, fraud and risk to the reputation of the university was a member of the university council. From the findings it can be noted that that there was a difference between the number of respondents who had knowledge of the existence of a person responsible for risk management procedures in place that cover the likely risks such as IT Risks, Occupational Health and Safety, environmental compliance, fraud and risk to the reputation of the university and if the person was a member of the council or not. This difference was as a result of respondents who simply answered yes to the question with no adequate knowledge because there is no official communication and notifications in the universities with regards to who is responsible. Only the councillors and principal officers had knowledge, that is, the 34% who knew if the person was the member of the council, that is the vice-chancellors whom are the chairpersons of these universities' risk committees reports to their respective councils on risk management and there are also ex-officio members, that is members of the council who are involved in the day to day running of the university.

VII. RISK ASSESSMENTS AND ANALYSIS

As regards to who carries out risk analysis and assessments in the universities, 47% of the respondents indicated that they had knowledge of who was responsible, that is, the risk committees. Sixty-nine (69%) indicated that they knew how many times does their university carry out risk assessments and analysis in a year, that is at least six (6) times which are the number of times the risk committees sit in a year.

RISK FRAMEWORKS

A considerable number of respondents, (44%), indicated that their university was using any enterprise risk frameworks in the form of a risk template which was designed by the risk committee. However, 56% of the respondents had no knowledge of the risk template because from document review of minutes and memos, it was noted that the template has only been adopted in the universities main committees. The template is not being used at department level and sub-committee level, that is, it has not been implemented, and hence there is little knowledge about it. Consequently no training was ever done so as to inform the university employees of the template and its significance, thus only employees who are members of main universities committees know about it.

IT AUDIT PROCESSES

As regards the number of times IT audit processes are carried out in various departments within the universities, 15% of the respondents indicated that in their departments they are done rarely once in two to three years. 66% had no idea if the audits are carried out or not and 19% indicated that IT audits have never been done in their departments.

IT RISK MANAGEMENT ON THE AGENDA OF COUNCIL MEETINGS

The councillors who returned our questionnaire noted that IT risk management is always on the agenda of council meetings by virtue that overall university risk management will be on the agenda and IT risk management is a sub-division of the university's risk management.

IT RISK MANAGEMENT AND COMPLIANCE STRATEGIES AND PROCEDURES AT UNIVERSITIES

As regards to the presence of an IT risk management strategy in the universities, 93% of the respondents indicated that they did not have any knowledge of its existence and the other 7% indicated that is present informally and it has been also implemented informally that is there is no paperwork or documentation about IT risk management in the universities. Three per cent (3%) of the respondents indicated that there are formal and written risk management procedures to cope with IT risks in the university, in the form of the university risk management strategy. The results show that, 89% of the respondents indicated that are there legal, regulatory, or policy requirements relative to delivery of the university's IT services and they have been implemented to some extent. The results also show that, 4% of the respondents knew that these procedures where implemented. The results also show that, 28% of the respondent indicated that the computer committees and the ITS directors were directly responsible for devising these procedures.

IMPLEMENTATION LEVEL OF IT RISK MANAGEMENT

Only two categories were chosen out of a possible four which were very large, large, limited and very low. The results of this study show that, 79% of the respondents said the universities' level of implementation of IT risk management and compliance was limited and 21% indicated that the level of IT risk management implementation in the university was very low. From the results of the study it was noted that the implementation is low to moderate because the way the culture of risk management is being enforced, the communication structure and process in the university and the absence of an IT policy.

CHALLENGES TO THE IMPLEMENTATION OF IT RISK MANAGEMENT

A reasonable number of the respondents (60%) acknowledged that there were setbacks like lack of an IT policy in the university, lack of documentation and literature on acceptable IT risk management, shortage of qualified personnel to guide the implementation of any identified mitigatory procedures and a ballooning student population that has made it impossible to fully monitor all the activities pertaining to IT risk management. To overcome these setbacks the universities need to develop an IT policy and the document should be communicated to all employees at every level.

VIII. DISCUSSION

The results of this research show that there is a risk management knowledge gap between the ordinary employees and the university management. There was a huge difference between the number of respondents who had knowledge of the existence of a person responsible for risk management procedures of the university and if the person was a member of the council or not. It was noted that the ordinary employees were not aware of this because there is no official communication and notifications in the university with regards to who is responsible. Only the councillors and principal officers were aware that the vice-chancellor, who is a council member and also the chairperson of the university's risk committee. To overcome this gap there is need to fully

notify employees on university structures and systems like the committee system so as to make them fully aware, through use of notices and documentation like year books, memos, newsletters, university websites and strategy documents.

IT risk management and compliance is being implemented haphazardly and no trainings have been conducted so as to increase awareness of IT risks and promote the use of the risk template, only the faculty heads have been involved but nothing much has been done to increase and promote risk awareness and use in university departments. The lack of an IT policy which is an administrative control for IT risk management is hindering the university in implementing proper IT strategies and as a result the university's IT resources are prone to abuse by employees as there are no guidelines to how the resources are supposed to be used and how can these resources be utilized so as to give the university leverage against its competitors. It turns out, in this study, that the university is using obsolete machines.

The universities are using a computerized and an in-house developed student registration, accounting and result processing system so as to reduce human errors. The absence of crafted policies and procedures to govern the use of these IT resources is a risk to the university and this risk will only be mitigated when there is an IT policy in the university. The university is enforcing the culture of risk management awareness, through creation of a risk management committee and its sub-committees which feed input into the main risk management committee, incorporating all faculty heads in the risk management committee with the hope that they will disseminate the proceedings from the risk management committee to their faculties and departments, through the use of a risk template that covers all risks in the university including IT risks, by ensuring that all the committees and sub-committees in the university completes the risk template for all their recommendations and through the use of documentation such as the risk template and the quality assurance policy.

However the culture has not been inculcated to all department as and employees as the findings noted that ordinary employees are still not aware of the existence of the risk template, university `risk strategies are not being communicated and there is no documentation and policies to enforce IT risk management. The university has to ensure flat communication structures and spread notifications through electronic and non-electronic means. Lack of awareness and education on the risk is also another challenge to the implementation of IT risk management, that is, from the findings of this study many IT users at do not have an appreciation of the benefits of IT risk management and compliance, and its impact. Strategies such as provision of useful guidelines that can assist in the creation of an effective risk awareness culture can be used. A flat decision-making, reporting and communication structure, in the university is critical for the implementation of a consistent, effective, and efficient IT policy which will encompasses IT risk management and compliance.

IX. RECOMMENDATIONS

The university councils should ensure that IT policies and plan for systems and processes of IT risk management has been developed. The councils should implement flat decision-making, reporting and communication structures. The researcher also recommends flat communication structures on developments and decision making so as to overcome the challenges to the implementation of IT risk management and compliance. The absence of crafted policies and procedures to govern the use of these IT resources is a risk to the universities' IT resources and also a challenge to the implementation of IT risk management and compliance. The researcher recommends the development of comprehensive IT policy which addresses IT risks, IT risk management and IT compliance issues. The university councils should monitor, assess and review the implementation and execution of this policy at least once a year. The IT policy should be widely distributed throughout the university in both hard and soft copy form.

The findings of the study established that there is a risk management knowledge gap between the university management and the employees. To overcome this gap, the researcher recommends that employees should be fully notified through on university structures and systems like the committee system so as to make them fully aware, through use of notices and documentation like year books, memos, newsletters, the university website and strategy documents. The researcher also recommends that the university management should consider establishing a compliance function through the establishment of effective communication structures and communication of key performance indicators relevant to IT risk management and compliance, risk education and training.

The researcher also recommends that the risk template should be publicised and it should be easily accessed by all employees. Issues and strategies of risk management should be communicated to all employees and not only to the top management only. The risk committee should communicate information that raises awareness about risk management and statutory compliance obligations, through the use of tools like the risk template, university

website for notices, the year book as the code of conduct and the university newsletter. The university's risk committee should also ensure that IT risks are adequately addressed and enforced through the risk template. The risk committee should also obtain appropriate assurance that controls are in place and effective in addressing IT risks. The researcher also recommends that the university's audit committee should consider IT as it relates to financial reporting and the going concern of the university. The audit committee should consider the use of technology to improve audit coverage and efficiency of IT risk management.

The risk awareness culture should encourage all staff to identify risks and associated opportunities and to respond to them with cost effective actions. Creating a risk awareness culture in the university is a crucial part of implementing and sustaining IT risk management and compliance programme. The induction and on-going training programmes of the university staff should incorporate IT risk governance and it should incorporate an overview of and any changes to applicable laws, rules, codes and standards. The universities' Information Technology Services (ITS) department in conjunction with the HR departments should develop training programs to educate all university employees about IT risk management and its benefits. By offering this training, the lack of understanding and low appreciation of IT risk management will be minimised and the knowledge will be used to effectively implement IT risk management and compliance.

X. CONCLUSION

Management security controls that focus on the stipulation of information protection policy, guidelines, and compliance standards, in conjunction with technical and operational controls which are carried out through operational procedures should be implemented to manage and reduce the risk of loss and to protect the universities' computer assets. If the universities implement the above recommendations they will be able to overcome the challenges to the implementation of IT risk management and compliance and they will become a model institutions for IT risk governance. In conclusion, The universities has to work towards the improvement of their IT risk management strategies so that they will be able to achieve their strategic goals through the use of IT risk management as a corporate strategy.

REFERENCES

[1] Bandyopadhyay, K, Mykytyn, P. P, & Mykytyn, K, 1999. A framework for intergrated risk management in information technology. USA: Management Decision.

[2] Bandyopadhyay, K, Mykytyn,P, and Mykytyn, K, 1999. A framework for intergrated risk management in information technology. USA: Management Decision.

[3] Blakley, B, McDermott, E & Geer, D, 2001. Information security is information risk management. California: ACM Press.

[4] Botha, E. e tal, 1991. Introduction to research in education, Durban: Butterworth.

[5] Boyd, H, 2004. Marketing Research. Delhi: Richard Irwin Inc.

[6] BS 7799-1, 1999. Information Security Management - Part 1: Code of practice for information security management. London: British Standards Institution.

[7] Caballero, T, Albert, C, 2009. Computer and Information Security Handbook. Elsevier: Morgan Kaufmann Publications Inc.

[8] Churchill, G, 2000. Marketing Research, Methodology and Foundations, 6th ed. Fort Worth, T`X: Drygen Press.

[9] COSO, 2004. Enterprise risk management framework. Available from: http:// www.coso.org

[10] Cule, P, Schmidt, R, Lyytinen, R & Keil, M, 2000. Strategies for Leading off IS Project Failure-Information Systems Management. UK: Spring.

[11] Deloitte and Touche, 2002. Management briefing - information security. Available from: http://www.deloitte.com/dtt/cda/doc/content/info security(1).pdf.

[12] ENISA, 2006. Risk management and Risk assessment inventory. United States of America: ENISA

[13] Flynn, I. M & McIver, A, 1997. Understanding operating systems, Second ed. United States of America: PWS Publishing.

[14] FoxT, 2011. IT Compliance, accepted standards and licensing. Delhi: New Richard Irwin Inc.

[15] Frosdick, S, 1997. The techniques of risk analysis are insufficient in themsleves. Disaster Prevention and Management. United States of America: International Journal.

[16] Frosdick, S, 1996. Practical management of programme risk: the case of the national strategy for police information systems for england and wales. England: Information Management and Computer Security.

[17] Frosdick, S, 1997. The techniques of risk analysis are insufficient in themsleves. Disaster Prevention and Management. London: Oxford Press.

[18] Furnas, D, R, 2004. Due care or do not care? Available from: http://www.issa-sac.org/info resources/Due Care 5-13-04.shtml.

[19] Gamma Secure Systems Limited, 1997. A practitioner's view of cramm. Available from: http://www.gammassl.co.uk/topics/hot.html: Gamma Secure Systems Limited.

[20] Gerber, M & von Solms, R, 2001. From risk analysis to security requirements. Computers and Security

[21] Gerber, M, & von Solms, R, 2005. Management of risk in the information age. Computers and Security

[22] Ghauri, P and Gronhaug, K, 2002. Research Methods in Business Studies. USA:Prentice Hall.

[23] Girard, K, 2002. Three big breakdowns of 2001. Available from: http://www.findarticles.com/p/articles/mi zdbln/is 200201/ai ziff21763.

[24] Grant, G. H, 2003. The evolution of corporate governance and its impact on modern corporate America. United States of America: Management Decision

[25] Heemstra, F, J and Kusters, R, J, 1996. Dealing with risk: A practical approach. United States of America: Journal of Information Technology.

[26] Hilmer P, 1993, IT governance. California: Pearson Hill

[27] Humphreys, E. J, Moses, R. H & Plate, E. A, 1998. Guide to BS7799 Risk Assessment and Management. London: British Standards Institution.
[28] Institute of Directors of Southern Africa, 2002. Corporate Governance. Available from: http://www.iodsa.co.za.
[29] IT Governance Institute, 2005. Information Risks : Whose Business are they?. ISBN 1-933284-10-2, Available from www.isaca.org
[30] Information Security Governance, 2005. It's your responsibility. retrieved from http://www.deloitte.com/dtt/cda/doc/content/UK_TA_Infosecurity_2005.pdf, April 2006
[31] Information Security and Corporate Governance. Available from: http://www.computerworld.com/securitytopics/security/story/0,10801,92915,00.html.
[32] ISACA, 2006. CISA Review Manual 2006-Information Systems Audit and Control Association. Rolling Meadows: ISACA
[33] ISACA, 2009. The Risk IT Framework. Rolling Meadows: ISACA
[34] ISO/IEC TR 13335-2, 1997. Guidelines for the management of IT security (GMITS) – part 2: Managing and planning IT security. USA: ISO/IEC.
[35] IT Governance Institute, 2003. Board Briefing on IT Governance. Available from: http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board Briefing on IT Governance/26904 Board Briefing final.pdf.
[36] IT Governance Institute, 2004. IT Strategy Committee. Available from: http://www.ITgovernance.org/resources.htm.IT Governance Institute, 2005. Information Security Governance: Guidance for Boards of Directors and Executive Management. Available from: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=15998.
[37] IT Governance Ltd, 2005. Board Briefing on IT Governance [online] viewed from <www.itgovernance.co.uk> [02 February 2012]
[38] ISO/IEC 38500:2008, 2007. Corporate governance of information technology. ISO/IEC. IT Governance Institute: COBIT 4.1. USA: ISACA, Rolling Meadows.
[39] Jennings, T, 2004. Change Management: An Essential Tool for IT Governance. Available from: http://www.merant.com/Shared/pdfs/dimensions/CM for IT Governance.pdf.
[40] Katsicas M, Sokratis K, 2009. Computer and Information Security Handbook. Elsevier: Morgan Kaufmann Publications Inc.
[41] King 2 Report on Corporate Governance, 2002, available from the Institute of Directors, Johannesburg, South Africa, www.iodsa.co.za
[42] King Report. The King 3 Report on Corporate Governance. Institute of Directors, Available from: http://www.iodsa.co.za/IoD
[43] Lewis, E & Millar, G, 2009. The viable governance model – a theoretical model for the governance of IT. Hawaii: HICSS
[44] Marczyk, G. DeMatteo, D. and Festinger, D, 2005. Essentials of Research Design and Methodology. New Jersey: John Wiley & Sons.
[45] Mayo, D & Hollander, R, 1991. Introduction to Part II – Uncertain Evidence in Risk Management. London: Oxford University Press.
[46] Michael E. Whitman and Herbert J. Mattford, 2003. Principles of Information Security. USA: Course Technology.
[47] Moeller, R, 2007.COSO Enterprise Risk Management. New Jersey: Wiley.
[48] National Computing Centre, 2005. IT Governance-Developing a Successful Governance Strategy. Manchester: The National Computing Centre.
[49] National Institute of Standards and Technology. 2001. NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. New York Stock Exchange: US Department of Commerce.
[50] The National Institute of Standards and Technology (NIST) and National Computer Security Center (NCSC), 2003. The Risk Management Research Laboratory Overview. Gaithersburg, MD: NIST and NCSC.
[51] Neuman, W, 2003. Social research methods: qualitative & quantitative approaches, 5th Ed. Boston, MA: Allyn and Bacon.
[52] Newell, F, 2000. www.Loyalty.Com. New York, NY McGraw-Hill.
[53] Nolan, R, 2004. Richard Nolan: A Committee of One's Own. Available from: http://www.cioinsight.com/article2/0,1397,1529279,00.asp.
[54] Oates, B, 2006. Researching Information Systems and Computing, London: Sage Publications
[55] OECD Principles of Corporate Governance, 2004, available from the OECD, www.oecd.org
[56] Payne, A. and Frow, P, 2005. A Strategic Framework for Customer Relationship Management. USA: Journal of Marketing.
[57] Rath, M & Sponholz, R, 2009. IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen. Berlin: Schmidt.
[58] Ritchie, B & Brindley, C, 2001. The information-risk conundrum. Marketing Intelligence and Planning.
[59] Tarantino A, Vu Broady D and Roland H.A, 2008. IT Risk management and compliance. Washington: WUC Press.
[60] Terry, S, 2000. Risk management: the need to set standards. Balance Sheet.
[61] US Commerce, 2003. Information Technology Risks. New York: US commerce Press.
[62] Von Solms B, 2006. What every vice-chancellor should know about ICT. Johannesburg: University of Johannesburg.
[63] Webb, S., & Robertson, M. (2004). Enabling IT Governance with Project Portfolio Management. Available from: http://itresearch.forbes.com/data/document.do?resid=1088617963 260.
[64] Whitman, M. E., & Mattord, H. J. (2003a). Principles of information security. In (pp.153 – 190). Course Technology.
[65] Wold, G. H., & Shriver, R. F. (Eds.). (1997). Risk analysis techniques.Available from: http://www.drj.com/new2dr/w3 030.htm: Systems Support, inc.
[66] Xactium, 2011. IT Compliance. New Jersey: John Wiley & Sons.