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*

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.