The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 11 || Pages || PP -01-06|| 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

An Analysis of the Information Security Governance in the State Owned Enterprises (Soe) In Zimbabwe.

Joseph Sigauke[1], Paul Mupfiga[2] , Theo Tsokota[2]

----------ABSTRACT----------
This study examined the existence and implementation of information security governance (ISG) in the state-owned-enterprises (SOE) in Zimbabwe. The study examined the implementation of information security governance in SOEs in Zimbabwe. This exploratory study was conducted using semi-structured interviews to collect data from a simple random sample. Interviews were also carried out with a composition of 13 Board members, 18 Executive management and 26 IT Executives. The data was then arranged into tables and for simple interpretation. The results of the study revealed that information security governance in SOE in Zimbabwe is still lagging behind. Despite the majority of Zimbabwe SOE recognizing the importance of ISG, most of them have no clear information security strategies or written information security policy statements. The study recommends that the state-owned-enterprises use IT governance frameworks such as COBIT, ITIL and BS17009.

Keywords - *Information security governance, State Owned Enterprise, Zimbabwe.*

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

I. INTRODUCTION

Information security refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, (USC-3542, 2011). This entails guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity of the information. This extends to preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information, and availability, which means ensuring timely and reliable access to and use of information. A secure system must satisfy some importance features: confidentiality, integrity, availability and accountability (Kumar, 1995). The level of satisfaction, or the confidence the system transmits, is defined by a security policy which creates rules of what area what are not allowed in the system. Security policies are important to the security management strategy. An SOE'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 SOE, (Tarantino et al, 2008). Information that is processed in almost all SOEs in Zimbabwe is either processed manually or electronically (involving the use of information technology (IT) equipment). At times the information is exchanged electronically using facilities such as the internet for file transfer or e-mails. These facilities provide fast exchange of information; they also possess great danger of divulging the information to the unintended recipients. Information about the organization may be compromised to the extent that it may be regarded as information espionage.

II. INFORMATION SECURITY GOVERNANCE (ISG)

ISG is defined as the organization's management responsibilities and practices that provide strategic vision ensure objectives are achieved, manage risks appropriately, use organizational resources responsibly, and monitor the success or failure of the information security programs (IBM Global Business Services, 2006). According to IBM (2006), ISG relates to the protection of valuable assets against loss, misuse, disclosure, or damage. In this context, valuable assets are the information recorded on, processed by, stored in, shared by, transmitted from, or retrieved from an electronic medium. The information must be protected against harm from threats leading to different types of impacts such as loss, inaccessibility, alteration, or wrongful disclosure. While there are many characteristics to IT security governance, an all-inclusive definition is difficult to contextualise. Leading practice dictates that IT security governance defines the core IT security principles, the accountabilities and actions of an organisation, to ensure that its objectives are achieved. IT governance provides outcomes specifically focused on aligning IT with the business while security governance provides