

ABSTRACT

The development of technology plays an important role in getting information especially with the internet, access to get information will be easier. Information is one of the important needs for companies to support decision making. Good management of information systems is needed if you want to manage information. The results of the management of information are confidential in nature which will require protection controls to minimize risks that can cause harm to the company. This study aims to conduct an information security risk assessment on ZZZ information systems in government agencies X. This research is a qualitative research with descriptive objectives. The data processing technique uses a combination of risk calculation and ISO / IEC 27005: 2011 document matrix and NIST SP 800-30 Revision 1 which is supported by triangulation theory.

The results of this study indicate that there are 24 risks that need to be mitigated while there are 29 risks accepted by government agencies X. The number of risks with a very low value of seven, low as much as 40, moderate as much as five. 25 types of threats were identified for each asset associated with the ZZZ information system, these types of threats originated from 19 sources of threats that have been considered. There are 22 controls in each asset.

Thus it can be concluded that government agency X needs to implement minimal information security risk management for internal circles in order to maintain confidentiality, availability and integrity (CIA). The data from this research can be used as material for further research to find out the actions on the risk of each asset by using other documents such as ISO 27002 and others.

Keywords: *Risk assessment, information security, ISO/IEC 27005:2011, NIST SP 800-30Revision1.*