BAYESIAN NETWORK AND COSINE SIMILARITY METHOD FOR SYSTEM IDENTIFICATION IN INFORMATION SECURITY CONTROL

By: Indri Sudanawati Rozas
Student Identity Number: 5109201045

ABSTRACT

Information security is a responsibility that cannot be easily considered. Besides many things must be calculated to ensure information security, type of information security threats and attack that always grow also has its own challenges. ISO 27001 or ISO 27001:2005 is a standard Information Security Management System (ISMS) which gives general overview of what should be done by company in order to implement the concepts of information security. There are 133 information security controls to safeguard company assets, but not all controls must be carried out. Companies can choose which controls are appropriate to the conditions. The selection is usually rely on information security consultant. Of course the using of consultant will increase the cost of its own.

This research builds a system that name SiPKoKI. SiPKoKI can give a recommendation of information security controls in accordance with threat data information that occurs within a company. Data information security threats that occur then represented in the structure of Bayesian network. From Bayesian network structure then SiPKoKI calculating the risk of information security threats (risk assessment) of each asset. Having obtained the value of the risk, then proceed by selecting security controls in the ISO 27001 information that best suits the threat occurred. The process of selecting the appropriate controls is using the cosine similarity method. SiPKoKI similarity mechanism is use the term adverse threat data on information security and terms contained in the document ISO 27001.

From the test of the system result obtains that SiPKoKI have 100% success to help calculate the risk value. While the resulting level of relevance to the recommendations based on ISO 27001 security control is 70% on standard terms and 90% in the extended term. Tests also get the result that the expansion of one term will increase the value of the cosine similarity by an average 0.04.

Key word: information security, ISO 27001, bayesian networks, cosine similarity, SiPKoKI, internal controls.