

ABSTRACT

Information technology currently plays an important role in supporting business processes and enhancing company competitiveness. The rapid development of information technology today makes information one of the most important and very valuable assets for companies. In health agencies, especially hospitals, there is a health information system that is built to integrate data and information management systematically at all levels of the health sphere, which greatly supports business and service operations. The presence of information technology is never separated from the potential threats and risks from various types and sources. Risks and threats that may occur can attack the aspects of information security, namely confidentiality, integrity and availability. So we need an approach to manage risk adequately, one of which is by implementing information technology risk management. This study aims to conduct risk assessment and analysis at RSUD Bayu Asih Purwakarta. This study uses a qualitative analysis with a case study method. Risk analysis uses the approach of the ISO / IEC 27005: 2011 standard as a framework for its information technology risk management. The research result states that there are 23 lists of information technology assets that need to be identified as asset value, threat level and impact level. The majority of the types of threats that may occur have a low level. It found 96 risks related to hospital information technology based on the type and level of threat for each asset, namely 9 risks with a medium level (medium risk), and 87 risks with a low level (low risk)

Keywords: information security, ISO / IEC 27005, risk management, information technology, hospital