ABSTRACT

The banking industry is one of the vital sectors for the economic growth of a country. This causes the banking sector to always be vulnerable to risk. Judging from the information security triad, every data and information, especially in the banking sector, must be able to guarantee its confidentiality, authenticity and availability. Sharia Banks have a CISO (Chief of Information Security Officer) department as an important department to carry out digital security for Islamic Banks. Seeing the massive practice of cyber security crimes will certainly increase a good understanding of the CISO dept. This will improve the general information management system. Make the organization better prepared to face, mitigate and make decisions in the future. Considering this, this research aims to be able to implement the ISO/IEC 27005:2018 framework or standard and assess risk using the FMEA (Failure Modes and Effect Analysis) method in the CISO department. The results of the research are in terms of risk in the CISO department of Islamic banks and mitigation documents for each threat and asset. Found about 45 risks that exist in the CISO department of Islamic banks. These risks can be categorized into Very High, High, Medium, Low and Very Low classes according to the RPN value. In this case there is neither very high nor high risk, only one moderate risk, 28 Low risk and sixteen Very Low risks. Islamic banks already have good and holistic security protection.

Keywords: Risk, Risk Management, assets, threats, ISO/IEC 27005:2018