ABSTRACT

Security Operation Center (SOC) is a security control center that focuses on monitoring, detection, analysis, and rapid response to cybersecurity threats. SOC aims to protect organizations from cyber attacks that can harm assets, reputation, and business. SOC has been implemented at PT Non-Bank Financial Company (NBFC) for the security of its information systems. However, PT NBFC still has problems, namely not having an impact analysis process on Financial and Regulatory Requirements and calculating the costs and efforts required for recovery from detected events/incidents, there are no Key Performance Indicators (KPIs) and Key Risk Indicators (KRI) set by management to monitor the effectiveness of physical access control and compliance with applicable standards, not having an official program related to insider threats (threats from within the organization). Therefore, this study evaluates the effectiveness of SOC in addressing information security threats at PT Non-Bank Financial Company (NBFC) using the ISO 27005:2018 and NIST SP 800-30 frameworks. The results of the study are the proposed guidance framework for SOC assessment, a combination of the ISO 27005:2018 and NIST SP 800-30 frameworks consisting of several stages of research assessment, risk assessment, risk treatment and risk acceptance strategy and monitoring. In addition, this study produces a maturity level assessment of the ISO 27005:2018 framework, NIST SP 800-30 and the proposed framework. From the maturity level assessment, the proposed framework achieves good maturity because there are 2 domains that reach the target maturity value and 1 domain that is already at level 4 - Managed and Measurable. In terms of the domains used in the new framework, it includes domains from ISO 27005:2018 and NIST SP 800-30 so that organizations can utilize a more comprehensive approach, involving strategic, managerial, and technical aspects of risk management.

Keywords: *Cyber Security, Maturity level, Non-Bank Financial Company, Security Operation Center (SOC), Information System*