ABSTRACT

PT. XYZ already has an Enterprise Risk Management (ERM) division to handle general risk management but has not yet implemented specific IT risk management. This study aims to evaluate the potential risks that may arise in the operations of PT. XYZ's IT division, as it currently lacks dedicated IT risk management. The research uses the ISO 27005 framework as the primary guide for risk management, while COBIT 2019 is utilized for risk identification and source of risk in this study. The researcher collects data through the distribution of questionnaires to gather information from the Expert Head Unit and IT Staff Unit regarding their views and experiences related to risk management and conducts in-depth interviews to validate the results from the questionnaires. The identification results revealed four risk profiles determined by PT. XYZ, with a total of 21 identified risks. This indicates that the IT division requires a comprehensive risk management approach to anticipate various threats and vulnerabilities that could impact IT operations and the company's continuity.

Keywords—Risk Management, Information Technology, ISO/IEC 27005, COBIT 2019