ABSTRACT

PT XYZ is a company specializing in Maintenance, Repair, and Overhaul (MRO). Although an Enterprise Risk Management (ERM) division is in place, there is currently no specialized approach for managing risks within the IT unit, which can lead to poorly managed IT risks and disrupt the company's operations. This study aims to evaluate the potential risks that may arise in the IT operations of PT XYZ and develop recommendations for effective risk management. The ISO 27005 framework is chosen as the standard for risk management, while risk identification is based on COBIT 2019 as a reference for the risk list used. Data were collected through questionnaires and interviews with relevant stakeholders. The study identified 23 risks, categorized as 8 Low, 7 Medium, 5 High, and 3 Crisis. Of these 23 risks, 15 will be addressed with control measures using the COBIT 2019 framework and additional guidance from NIST SP-800-53. These steps are intended to ensure that the risks are managed effectively, with the goal of enhancing the operational efficiency of PT XYZ's IT division. Consequently, this research is expected to assist PT XYZ in minimizing potential operational disruptions and ensuring better business continuity.

*Keywords—**Risk Management, Information Technology, ISO 27005, COBIT 2019***