ABSTRAK

Ketiadaan kerangka kerja formal untuk pengelolaan risiko keamanan informasi membuat perusahaan rentan terhadap gangguan operasional yang signifikan serta potensi kerugian finansial. Penelitian ini bertujuan untuk melakukan penilaian risiko secara sistematis pada PT XYZ berdasarkan aset teknologi informasi yang dimiliki, dengan mengacu pada standar ISO/IEC 27005:2022. Metode penelitian mencakup beberapa tahapan, yaitu penetapan konteks untuk menentukan kriteria risiko, serta identifikasi risiko untuk memetakan 31 aset TI, ancaman, dan kerentanan yang terkait. Analisis dan evaluasi risiko dilakukan untuk menentukan tingkat risiko dan prioritas penanganan yang diperlukan. Hasil penilaian mengidentifikasi total 265 skenario risiko, dengan profil risiko perusahaan terdiri dari 10 risiko tingkat *High* (3,77%), 68 risiko tingkat *Medium* (25,66%), dan 187 risiko tingkat *Low* (70,57%). Berdasarkan hasil evaluasi, rencana penanganan risiko merekomendasikan modifikasi risiko untuk seluruh skenario dengan rekomendasi kontrol yang diadaptasi dari ISO/IEC 27001:2022. Penelitian ini menyimpulkan bahwa penerapan kerangka kerja ISO/IEC 27005:2022 efektif dalam memberikan peta risiko yang komprehensif serta rencana prioritas mitigasi yang terstruktur. Hasil penelitian ini diharapkan dapat menjadi panduan praktis bagi organisasi serupa dalam membangun fondasi manajemen keamanan informasi yang objektif dan efisien.

Kata Kunci: ISO/IEC 27005:2022, ISO/IEC 27001:2022, manajemen risiko keamanan informasi, aset teknologi informasi

ABSTRACT

The absence of a formal framework for managing information security risks makes companies vulnerable to significant operational disruptions and potential financial losses. This study aims to systematically assess risks at PT XYZ based on its information technology assets, referring to the ISO/IEC 27005:2022 standard. The research method includes several stages, namely context establishment to define risk criteria, and risk identification to map 31 IT assets, threats, and vulnerabilities. Risk analysis and evaluation were conducted to determine the level of risk and prioritize appropriate treatment. The assessment identified a total of 265 risk scenarios, with the company's risk profile consisting of 10 High-level risks (3.77%), 68 Medium-level risks (25.66%), and 187 Low-level risks (70.57%). Based on the evaluation results, the risk treatment plan recommends risk modification for all scenarios with control recommendations adapted from ISO/IEC 27001:2022. This study concludes that implementing the ISO/IEC 27005:2022 framework is effective in providing a comprehensive risk map and a structured mitigation priority plan. The findings are expected to serve as a practical guide for similar organizations in establishing an objective and efficient information security management foundation.

Keyword: ISO/IEC 27005:2022, ISO/IEC 27001:2022, *information security risk management, information technology assets*