

ABSTRAK

Penelitian ini bertujuan untuk melakukan analisis risiko keamanan informasi pada sistem kredit BPR Nusamba Banguntapan dengan mengadopsi kerangka kerja ISO/IEC 27005:2022. Analisis dilakukan melalui identifikasi aset informasi, menganalisis tingkat kemungkinan dan dampak risiko, serta menyusun rekomendasi mitigasi risiko. Penelitian menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus. Pengumpulan data dilakukan melalui observasi, wawancara semi-terstruktur dengan Kepala Bidang Kepatuhan, studi dokumen, dan studi literatur. Penilaian risiko dilaksanakan sesuai kerangka ISO/IEC 27005:2022 yang mencakup penetapan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, dan penanganan risiko. Hasil penelitian mengidentifikasi 25 aset informasi, 21 jenis ancaman, dan 37 kerentanan, dan 67 skenario risiko. Hasil evaluasi risiko menunjukkan 1 risiko berada pada kategori sangat rendah, 25 risiko berada pada kategori rendah, dan 40 risiko berada pada kategori sedang. Seluruh skenario risiko direkomendasikan untuk ditangani melalui strategi modifikasi risiko berdasarkan kontrol ISO/IEC 27001:2022 Annex A. Hasil penelitian diharapkan dapat menjadi acuan BPR dalam meningkatkan pengelolaan risiko TI dan keamanan informasi.

Kata kunci: ISO/IEC 27005:2022, keamanan informasi, penilaian risiko, BPR, sistem kredit

ABSTRACT

This study aims to conduct an information security risk analysis of the credit system at BPR Nusamba Banguntapan by adopting the ISO/IEC 27005:2022 framework. The analysis was conducted by identifying information assets, analyzing the likelihood and impact of risks, and formulating risk mitigation recommendations. The study employed a descriptive qualitative approach using the case study method. Data collection was conducted through observation, semi-structured interviews with the Head of the Compliance Division, document review, and literatur review. Risk assessment was carried out in accordance with the ISO/IEC 27005:2022 framework, which includes context establishment, risk identification, risk analysis, risk evaluation, and risk treatment. The study identified 25 information assets, 21 type of threats, and 37 vulnerabilites, resulting in 67 risk scenarios. The risk evaluation results showed that 1 risk was in the very low category, 25 risks were in the low category, and 40 risks were in the medium category. It was recommended that all risk scenarios be addressed through risk mitigation strategies based on the controls in ISO/IEC 27001:2022 Annex A. The research results are expected to serve as a reference for BPR in improving IT risk management and information security.

Keywords: ISO/IEC 27005:2022, information security, risk assessment, BPR, credit system