



INTISARI

Risiko dalam pengelolaan keamanan informasi perlu ditangani secara sistematis dan terstruktur agar organisasi dapat meminimalkan potensi kerugian dan menjaga keberlangsungan operasional. Standar SNI-ISO 31000 memberikan panduan umum dalam manajemen risiko, yang dalam penelitian ini diterapkan pada pengembangan aplikasi Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan ISO 27001:2022. Penelitian ini bertujuan untuk merancang, mengembangkan, dan menguji fungsionalitas sistem manajemen risiko berbasis standar tersebut.

Metodologi yang digunakan meliputi perancangan sistem berdasarkan standar ISO dan *Unified Modelling Language* (UML), pengembangan menggunakan pendekatan *Software Development Life Cycle* (SDLC) model *agile*, serta pengujian fungsionalitas melalui metode *blackbox testing* untuk memastikan seluruh fitur berjalan sebagaimana mestinya. Fitur utama yang dikembangkan mencakup proses identifikasi, penilaian, penanganan, dan penerimaan risiko, serta penyusunan dokumen dan pernyataan keberlakuan kontrol. Hasil pengujian menunjukkan bahwa seluruh fitur berfungsi dengan baik, dengan tingkat keberhasilan fungsionalitas mencapai 100%.

Selain itu, uji pengalaman pengguna dilakukan di lingkungan Dinas Komunikasi, Informatika dan Persandian (Diskominfo Sandi) Kota Yogyakarta untuk menilai efektivitas sistem. Survei menunjukkan bahwa aplikasi dinilai cukup efektif dalam mendukung implementasi manajemen risiko berbasis SNI-ISO 31000 di lingkungan SMKI, dengan 25% responden memberikan skor 4 dari 5, dan 75% memberikan skor 5 dari 5. Dengan demikian, sistem ini terbukti mampu mendukung proses manajemen risiko secara efektif dan dapat dijadikan alat bantu yang sesuai standar. Namun, perlu dicatat bahwa pengujian hanya dilakukan pada satu instansi, sehingga pengujian lanjutan di sektor atau organisasi lain masih diperlukan untuk menilai sejauh mana aplikasi dapat beradaptasi dan memberikan manfaat secara konsisten.

Kata Kunci: manajemen risiko, ISO 31000, keamanan informasi, aplikasi berbasis web, ISO 27001



ABSTRACT

Risks in information security management must be addressed systematically and structurally so that organizations can reduce potential losses and maintain operational continuity. The SNI-ISO 31000 standard provides general guidelines for risk management, which in this study is applied within the scope of an Information Security Management System (ISMS) application in accordance with ISO 27001:2022. This study aims to design, develop, and test the functionality of a risk management system based on these standards.

The methodology includes system design using ISO-based approaches and Unified Modeling Language (UML), application development using the Software Development Life Cycle (SDLC) with an agile model, and functionality testing using the blackbox testing method to ensure that all features work as expected. The main features of the system include risk identification, risk assessment, risk treatment, risk acceptance, as well as document generation and the Statement of Applicability (SoA) control module. The testing results showed that all features functioned properly, achieving a 100% success rate in functionality testing.

In addition, user experience testing was conducted at the Department of Communication, Informatics, and Encryption (Diskominfo Sandi) of Yogyakarta City to evaluate the system's effectiveness. The survey showed that the application's effectiveness in supporting the implementation of risk management based on SNI-ISO 31000 within the ISMS based on SNI-ISO 27001 was considered satisfactory, with 25% of respondents giving a score of 4 out of 5, and 75% giving a score of 5 out of 5. Therefore, the system has proven to effectively support the risk management process and can serve as a standards-based tool for implementing risk management in the ISMS domain. However, it should be noted that testing was only carried out in one institution, so further testing in other sectors or organizations is recommended to evaluate how well the application can adapt and consistently provide benefits.

Keywords: risk management, ISO 31000, information security, web-based application, ISO 27001