ANALISIS MANAJEMEN RISIKO PADA SISTEM INFORMASI MANAJEMEN RUMAH SAKIT (SIMRS) DENGAN ISO 31000 DAN NIST 800-30 DI RSUD H. OK ARYA ZULKARNAIN

ABSTRAK

Sistem Informasi Manajemen Rumah Sakit (SIMRS) merupakan sistem terintegrasi yang mendukung pelayanan, administrasi, dan pengelolaan data di rumah sakit. Namun, penerapannya tidak terlepas dari berbagai risiko yang dapat memengaruhi operasional dan keamanan informasi. Penelitian ini bertujuan untuk menganalisis manajemen risiko pada SIMRS di RSUD H. Ok Arya Zulkarnain dengan menggabungkan dua kerangka kerja, yaitu ISO 31000 dan NIST 800-30. ISO 31000 digunakan untuk identifikasi risiko secara umum, sedangkan NIST 800-30 berfokus pada aspek keamanan informasi dan terdapat pengujian sistem menggunakan aplikasi Acunetix. Hasil penelitian menunjukkan terdapat 15 risiko yang diklasifikasikan ke dalam tiga kategori: lima risiko tergolong *high* yaitu *human error* (kesalahan dalam mengoperasikan sistem), kurang baiknya kualitas jaringan, listrik padam, terserang virus atau *malware* pada *software* dan penyalahgunaan hak akses. Delapan risiko berada di tingkat *medium* yaitu *overload* sistem, *data corrupt*, *server down*, kerusakan *hardware*, pencurian perangkat keras, *cross-site request forgery (csrf),* petir dan kebakaran. Dua risiko lainnya, yaitu *header content-type* yang tidak ditetapkan dan *link* rusak dalam sistem, berada pada kategori low. Langkah-langkah mitigasi disusun berdasarkan hasil analisis risiko dan rekomendasi kontrol sesuai prinsip ISO 31000 dan NIST 800-30. Penelitian ini memberikan kontribusi dalam penyusunan strategi pengendalian risiko SIMRS secara terstruktur dan aplikatif untuk mendukung keberlangsungan sistem informasi manajemen rumah sakit.

Kata kunci: Manajemen Risiko, Sistem Informasi Manajemen Rumah Sakit (SIMRS), ISO 31000, NIST 800-30.

ANALISIS MANAJEMEN RISIKO PADA SISTEM INFORMASI MANAJEMEN RUMAH SAKIT (SIMRS) DENGAN ISO 31000 DAN NIST 800-30 DI RSUD H. OK ARYA ZULKARNAIN

ABSTRACT

Hospital Management Information System (SIMRS) is an integrated system that supports services, administration, and data management in hospitals. However, its implementation is not free from various risks that can affect operations and information security. This study aims to analyze risk management in SIMRS at RSUD H. Ok Arya Zulkarnain by combining two frameworks, namely ISO 31000 and NIST 800-30. ISO 31000 is used for general risk identification, while NIST 800-30 focuses on information security aspects and there is system testing using the Acunetix application. The results of the study showed that there were 15 risks classified into three categories: five risks were classified as high, namely human error (errors in operating the system), poor network quality, power outages, viruses or malware on software and misuse of access rights. Eight risks were at the medium level, namely system overload, data corruption, server down, hardware damage, hardware theft, cross-site request forgery (csrf), lightning and fire. The other two risks, namely undefined content-type headers and broken links in the system, are in the low category. Mitigation steps are prepared based on the results of risk analysis and control recommendations according to the principles of ISO 31000 and NIST 800-30. This study contributes to the preparation of a structured and applicable SIMRS risk control strategy to support the sustainability of the hospital management information system.

Keywords: Risk Management, Hospital Management Information System (SIMRS), ISO 31000, NIST 800-30.