

MANAJEMEN RISIKO KEAMANAN *INTEGRATED LIBRARY SYSTEM* MENGGUNAKAN METODE NIST SP 800-30 DAN KONTROL ISO/IEC 27001:2013

(Studi Kasus: *Integrated Library System*)

ABSTRAK

Penerapan teknologi informasi yang tepat dapat memberikan dampak baik pada proses bisnis organisasi maupun instansi pemerintah. Teknologi informasi membuat proses bisnis menjadi efektif dan efisien, sehingga menghasilkan keuntungan lebih besar, salah satu instansi pemerintah yang menerapkan teknologi informasi sebagai kegiatan operasional sehari-hari adalah Dinas Perpustakaan dan Kearsipan Daerah (DPKD) Kabupaten Sambas. DPKD Kabupaten Sambas menerapkan *Integrated Library System* dalam pengelolaan informasi dan pelayanan perpustakaan, namun DPKD Kabupaten Sambas belum melakukan manajemen risiko pada *Integrated Library System* yang merupakan aset penting dan belum mempunyai dokumen perancangan sistem manajemen keamanan informasi untuk memantau dan menanggapi ancaman pada *Integrated Library System*. Maka dari itu, penelitian ini dilakukan guna menganalisis dan menilai risiko keamanan pada *Integrated Library System* menggunakan metode NIST SP 800-30 Revisi 1 dan Kontrol ISO/IEC 27001:2013. Metode NIST SP 800-30 Revisi 1 dirancang sebagai analisis keamanan dalam memenuhi kebutuhan pemilik sistem dan profesional teknis untuk mengidentifikasi, menilai, serta mengelola risiko yang terdapat pada sistem. Kontrol ISO/IEC 27001:2013 terkandung persyaratan untuk mengontrol keamanan informasi yang disesuaikan dengan kebutuhan. Hasil penelitian berupa ancaman-ancaman yang bersumber dari *adversarial*, *accidental*, *structural* dan *environmental*, terdapat 3 risiko *adversarial* yang berada pada kategori tinggi dan sedang, 4 risiko *accidental* pada kategori tinggi dan sedang, 14 risiko *structural* pada kategori sangat tinggi, tinggi, sedang dan rendah, 3 risiko *environmental* pada kategori sedang dan rendah. Penelitian ini juga memberikan rekomendasi mitigasi keamanan yang diterapkan sesuai dengan permasalahan, ancaman dan kerentanan yang timbul terhadap *Integrated Library System*

Kata Kunci: Manajemen Risiko, Keamanan Informasi, NIST SP 800-30 Revisi 1, Kontrol ISO/IEC 27001:2013, *Integrated Library System*

INTEGRATED LIBRARY SYSTEM SECURITY RISK MANAGEMENT USING NIST SP 800-30 METHOD AND ISO/IEC 27001:2013 CONTROLS

(Case Study: Integrated Library System)

ABSTRACT

The application of the right information technology can have an impact on both the business processes of organizations and those of government agencies. Information technology makes business processes effective and efficient, resulting in greater profits. One government agency that applies information technology as a daily operational activity is the Sambas District Library and Archives Service (DPKD). Sambas District DPKD implements the Integrated Library System in information management and library services, but Sambas District DPKD has not implemented risk management on the Integrated Library System, which is an important asset, and does not yet have an information security management system design document to monitor and respond to threats to the Integrated Library System. Therefore, this research was conducted to analyze and assess security risks in the Integrated Library System using NIST SP 800-30 Rev. 1 and ISO/IEC 27001:2013 Control Methods. The NIST SP 800-30 Rev. 1 method is designed as a security analysis to meet the needs of system owners and technical professionals to identify, assess, and manage the risks inherent in the system. ISO/IEC 27001:2013 controls contain requirements to control information security according to needs. The results of the research are in the form of threats originating from adversarial, accidental, structural, and environmental sources. There are 3 adversarial risks in the high and medium categories, 4 accidental risks in the high and medium categories, 14 structural risks in the very high, high, medium, and low categories, and 3 environmental risks in the medium and low categories. This research also provides security mitigation recommendations that are applied in accordance with the problems, threats, and vulnerabilities that arise against the Integrated Library System.

Keywords: Risk Management, Information Security, NIST SP 800-30 Revision 1, ISO/IEC 27001:2013 Control, Integrated Library System