Pengembangan Kerangka Kerja Manajemen Risiko Keamanan Informasi Berdasarkan ISO/IEC 27005:2018 (Studi Kasus: Aplikasi Pengelolaan Data ABC di Institusi XYZ) = The Development of Risk Management Framework on the basis of ISO/IEC 27005:2018: a Case Study on Data Processing App at XYZ Institution

Endro Joko Wibowo, author

Abstrak

Keamanan informasi menjadi perhatian penting bagi pemerintah dan industri karena meningkatnya serangan siber selama Covid-19. Pemerintah dalam menyelenggarakan Sistem Pemerintahan Berbasis Elektronik (SPBE) Peraturan Presiden Republik Indonesia Nomor 95 tahun 2018 berkewajiban menjamin kerahasiaan, keutuhan, ketersediaan, keaslian dan kenirsangkalan sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE. Untuk mengatasi masalah tersebut pemerintah membutuhkan pendekatan untuk implementasi pengelolaan risiko keamanan informasi dan kontrol keamanan informasi. Penelitian ini bertujuan untuk melakukan risk identification, risk analysis, risk evaluation, risk treatment, risk acceptance, pengendalian risiko, menyusun kerangka kerja manajemen risiko keamanan informasi dan menilai kematangan Cyber security maturity pada domain tata kelola, identifikasi, proteksi, deteksi dan respon. Metodologi menggunakan ISO/IEC 27005:2018 sebagai panduan melakukan risk assesment. Kode praktik untuk kontrol keamanan informasi menggunakan standar ISO/IEC 27002:2013 dan menilai kematangan siber menggunakan model cyber security matury versi 1.10 yang dikembangkan oleh Badan Siber dan Sandi Negara Republik Indonesia. Dari hasil penelitian didapatkan bahwa penilaian risiko dan pengendalian risiko dengan dua metode yang digunakan dapat meningkatkan nilai kematangan siber organisasi dari 3.19 menjadi 4.06. Hasil penelitian ini juga menunjukkan bahwa kerangka kerja manajemen risiko keamanan informasi aplikasi pengelolaan data ABC telah sesuai dengan kebutuhan Institusi XYZ dalam menjalankan proses bisnisnya.

.....Information security is an important concern for the government and industry due to cyber attacks during Covid-19. The government in implementing the Electronic-Based Government System (SPBE) Presidential Regulation of the Republic of Indonesia Number 95 of 2018 guarantees the confidentiality, integrity, availability, authenticity and denial of resources related to data and information, SPBE Infrastructure, and SPBE Applications. To overcome these problems, the government in the approach to the implementation of information security risks and information security controls. This study aims to carry out risk identification, risk analysis, risk evaluation, risk treatment, risk acceptance, risk control, developing an information security risk management, and evaluation of cyber ââsecurity maturity, governance domain maturity, examination, protection, detection and response. The methodology uses ISO/IEC 27005:2018 as a guide for conducting a risk assessment. The code of practice for information security control uses the ISO/IEC 27002:2013 standard and assesses cyber maturity using the cyber security maturity model version 1.10 developed by the National Cyber ââand Crypto Agency of the Republic of Indonesia. From the results of the study, it was found that risk assessment and risk control with the two methods used can improve the cyber quality of the organization from 3.19 to 4.06. The results of this study also show that the security risk management framework for the application of ABC data management application is in accordance with the

needs of XYZ Institution in carrying out its business processes.