Universitas Indonesia Library >> UI - Tugas Akhir

Perancangan Kriteria Audit Keamanan Informasi Siber pada Sistem Informasi Manajemen Kepegawaian (SIMPEG): Studi Kasus Lembaga XYZ = Designing Cyber Information Security Audit Criteria for the Personnel Management Information System (SIMPEG): Case Study of XYZ Institution

Anisa Hermawati, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=9999920566061&lokasi=lokal

---

Abstrak

Sektor administrasi pemerintahan menjadi target utama peretasan. Kondisi ini cukup mengkhawatirkan mengingat kementerian dan lembaga (K/L) mengelola data sensitif, termasuk data profil Aparatur Sipil Negara (ASN). Lembaga XYZ menggunakan aplikasi internal Sistem Informasi Manajemen Kepegawaian (SIMPEG) yang dikembangkan oleh Unit Kerja Pusat Data dan Informasi (Pusdatin). Aplikasi SIMPEG wajib memenuhi standar teknis dan keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) sesuai dengan peraturan yang berlaku. Tujuan dari penelitian ini adalah merancang kriteria audit keamanan informasi siber untuk aplikasi SIMPEG dengan Perban BSSN Nomor 4 Tahun 2021, yang dikembangkan dengan standar keamanan informasi ISO/IEC 27001 dan kerangka kerja National Institute of Science and Technology (NIST) Cybersecurity Framework 2.0. Selain itu, penelitian ini juga bertujuan untuk mengevaluasi kondisi keamanan informasi siber aplikasi SIMPEG saat ini melalui pelaksanaa audit menggunakan kriteria yang telah dirancang, serta memberikan rekomendasi berdasarkan hasil audit tersebut. Penelitian ini menggunakan pendekatan kualitatif melalui deskripsi, analisis, interpretasi, dan perbandingan data yang dikumpulkan melalui wawancara, observasi, dan studi dokumen. Hasil dari penelitian ini adalah kriteria audit keamanan informasi siber dengan 133 pertanyaan yang mencakup aspek tata kelola dan manajemen serta fungsionalitas kinerja aplikasi. Kriteria ini juga dirancang sesuai prinsip perlindungan data pribadi dan karakteristik aplikasi SIMPEG. Audit yang dilakukan menunjukkan beberapa area yang perlu peningkatan, yaitu manajemen sesi, kriptografi, pencatatan log, keamanan komunikasi, serta pengelolaan file. Rekomendasi dari hasil penelitian ini yaitu pelatihan teknis keamanan informasi, menggunakan enkripsi data serta peningkatan security awareness.

.....The government administration sector is the main target of hacking. This condition is alarming considering that ministries and institutions (K / L) manage sensitive data, including the State Civil Apparatus (ASN) profile data. XYZ Institution uses the internal application of the Personnel Management Information System (SIMPEG) developed by the Data and Information Center Work Unit (Pusdatin). The SIMPEG application must meet the Electronic-Based Government System (SPBE) 's technical and security standards per applicable regulations. The purpose of this research is to design cyber information security audit criteria for the SIMPEG application with BSSN Regulation No. 4 of 2021, which was developed with the ISO/IEC 27001 information security standard and the National Institute of Science and Technology (NIST) Cybersecurity Framework 2.0 framework. In addition, this research also aims to evaluate the current state of SIMPEG application cybersecurity by conducting an audit using the criteria that have been designed and providing recommendations based on the audit results. This research uses a qualitative approach through description, analysis, interpretation, and comparison of data collected through interviews, observations, and document studies. This research results in a cyber information security audit criteria with 133 questions

covering aspects of governance and management as well as application performance functionality. These criteria are also designed according to the principles of personal data protection and the characteristics of the SIMPEG application. The audit showed several areas that need improvement, namely session management, cryptography, logging, communication security, and file management. Recommendations from the results of this study are information security technical training, using data encryption, and increasing security awareness.