Perancangan Manajemen Risiko Keamanan Informasi Sistem Informasi Manajemen Keimigrasian = Information Security Risk Management Design of Immigration Management Information System

Rina Rahmawati, author

Abstrak

Ditjen. Imigrasi sebagai pelaksana tugas dan fungsi Kementerian Hukum dan HAM RI di bidang keimigrasian telah memanfaatkan SI/TI yang mengintegrasikan seluruh fungsi keimigrasian baik di dalam maupun luar negeri, yaitu dengan Sistem Informasi Manajemen Keimigrasian (SIMKIM). Lingkup SIMKIM yang meliputi hampir seluruh aspek layanan keimigrasian menyebabkan ketersediaan layanan SIMKIM menjadi sangat penting. Tidak tersedianya layanan SIMKIM menyebabkan proses pelayanan keimigrasian menjadi tidak berjalan. Terjadinya insiden terkait keamanan informasi dalam organisasi serta maraknya kasus serangan siber di instansi pemerintah Indonesia, menuntut kepastian pengamanan SIMKIM untuk melindungi data krusial yang dimiliki. Tingginya ketergantungan Imigrasi terhadap SIMKIM dan dalam rangka menjaga kredibilitas instansi, dibutuhkan suatu perencanaan manajemen risiko keamanan informasi untuk menjamin kerahasiaan, integritas, dan ketersediaan layanan SIMKIM.

Dalam menyusun perencanaan manajemen risiko keamanan informasi SIMKIM, penelitian dilakukan dengan menggunakan kerangka kerja ISO/IEC 27005:2018 sebagai kerangka kerja utama dalam proses manajemen risiko, NIST SP 800-30 Rev. 1 sebagai panduan pelaksanaan aktivitas penilaian risiko, dan NIST SP 800-53 Rev. 5 sebagai acuan penentuan rekomendasi. Dari penilaian risiko, diidentifikasi 23 skenario risiko yang perlu dimitigasi oleh organisasi dan 5 skenario risiko yang dapat dialihkan ke pihak ketiga. Penelitian ini menghasilkan dokumen rancangan manajemen risiko keamanan informasi SIMKIM. .....The Directorate General of Immigration as the executor of the duties and functions of the Ministry of Law and Human Rights of Republic of Indonesia in the Immigration sector has utilized IS/IT that integrates all immigration functions both at inside and outside territory of Indonesia, namely the Sistem Informasi Manajemen Keimigrasian (SIMKIM). The scope of SIMKIM which covers almost all aspects of immigration services makes the availability of SIMKIM services very important. The unavailability of SIMKIM services causes the immigration service process to not work. The occurrence of incidents related to information security within the organization as well as the rise of cases of cyber attacks in Indonesian government agencies, demands the certainty of SIMKIM security to protect the crucial data held. Immigration's high dependence on SIMKIM and to maintain the credibility of the agency, an information security risk management plan is needed to ensure the confidentiality, integrity, and availability of SIMKIM services.

In preparing the information security risk management plan for SIMKIM, the research uses the ISO/IEC 27005 framework as the main framework in the risk management process, NIST SP 800-30 Rev. 1 as a guide for the implementation of risk assessment activities, and NIST SP 800-53 Rev. 5 as a reference for determining recommendations. From the risk assessment, 23 risk scenarios were identified that need to be mitigated by the organization and 5 risk scenarios that can be transferred to third parties. This research

produces a SIMKIM information security risk management design document.