

Penilaian Risiko Keamanan Informasi: Studi Kasus Sistem Informasi Pengembangan Kompetensi Aparatur Sipil Negara (SIPKA) Lembaga Administrasi Negara (LAN) = Information Security Risk Assessment: A Case Study of National Institute of Public Administration Civil Servants Competency Development Information System

Pamuji Lasiyanto Putro, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20503215&lokasi=lokal>

Abstrak

ABSTRAK

Lembaga Administrasi Negara (LAN) memiliki fungsi salah satunya pembinaan di bidang pengembangan kompetensi Aparatur Sipil Negara (ASN) mulai dari akreditasi lembaga pelatihan ASN sampai dengan pembinaan pelatihan kompetensi manajerial pegawai ASN. Untuk menunjang fungsi tersebut Lembaga Administrasi Negara menerapkan Sistem Informasi Pengembangan Kompetensi ASN (SIPKA). Layanan yang diberikan melalui SIPKA antara lain pemberian kode registrasi, akreditasi lembaga pelatihan untuk melakukan pembinaan terhadap penyelenggara pelatihan, dan pengembangan kompetensi ASN untuk menghasilkan informasi kinerja setiap instansi dalam pemenuhan hak pengembangan kompetensi ASN. Dalam operasionalnya, SIPKA beberapa kali terjadi insiden terkait keamanan informasi. Oleh karena itu diperlukan suatu penilaian risiko keamanan informasi serta langkah-langkah penanganan terhadap risiko yang timbul akibat insiden tersebut untuk mencegah terjadinya kebocoran informasi dan tetap tersedianya layanan informasi pada SIPKA. Penelitian ini dilakukan dengan tujuan untuk mengetahui tingkat risiko keamanan informasi pada SIPKA. Kerangka kerja yang digunakan pada penelitian ini berdasarkan pada standar ISO 27005. Penilaian risiko memiliki peranan penting, sejauh mana risiko yang ada pada SIPKA dan bagaimana penanganan risiko tersebut. Hasil yang diperoleh dari penelitian ini adalah profil risiko aplikasi SIPKA. Dalam profil risiko tersebut terdapat 20 skenario risiko yang ditemukan. Rincian dalam profil risiko terdapat 13 skenario risiko dimitigasi dengan menerapkan kontrol untuk mengurangi dampak atau kemungkinan terjadinya risiko, sedangkan tujuh skenario risiko lainnya diterima. Rekomendasi kontrol yang digunakan mengacu kepada standar ISO 27002.

<hr><i>ABSTRACT</i>

One of NIPAs (National Institute of Public Administration) function is to guide competence development of civil servants in form of civil servants training institution accreditation and civil servants managerial competency training. To support that function, NIPA develop the civil servants competency development information system. The system serves in providing registration code, accreditation of state civil apparatus training institution to produce performance information of those apparatus competency development rights. In its operation, the system has experienced incidents related to information security. Related to that incident, it is needed to develop an information security risk assessment and steps for handling risks caused by the incidents to prevent information leakage and keep information services available at the system. This research was conducted to find out level of information security risk in the system. The framework used in this study is based on ISO standard 27005. Risk assessment has an important role to figure out extent of the risk found in the system and how to handle the risk. Result of this research is risk profile. In the risk profile, there are 20 risk scenarios found. From the scenario of incident, there are 13 risk incident mitigated by

control to reduce the likelihood or impact of risk occurrence, while seven risks are accepted. Control recommendation to reduce risks are based on ISO 27002.