

Pengembangan Disain Mitigasi Risiko pada Otoritas Sertifikat Digital Pengadaan Barang/Jasa Secara Elektronik (OSD PSE) Berbasis COBIT 5 for Risk dan NIST SP 800-30 Revisi 1: Studi Kasus Balai Sertifikasi Elektronik = Development of Risk Mitigation Design at The Authority for Digital Procurement Certification (OSD PSE) Based on COBIT 5 for Risk and NIST SP 800-30 Revision 1: Case Study in Balai Sertifikasi Elektronik

Yulandi, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20481840&lokasi=lokal>

Abstrak

ABSTRAK

Di Indonesia, pihak yang berwenang untuk melakukan sertifikasi pengadaan secara elektronik adalah Otoritas Sertifikat Digital Pengadaan Secara Elektronik (OSD PSE) yang dikelola oleh unit kerja di Badan Sandi dan Siber Negara. OSD PSE memberikan jaminan layanan keamanan pada pengadaan secara elektronik di banyak sektor. Penelitian ini difokuskan pada identifikasi, analisis dan respon risiko layanan OSD PSE untuk mendapatkan enabler process dan Key risk indicator dengan mengkombinasikan metode Risk Scenario COBIT 5 dan NIST SP 800-30 Revision 1. Berdasarkan hasil penelitian diperoleh 14 enabler proses yaitu APO07.01, APO07.03, APO07.06, DSS01.01, DSS01.04, DSS05.05, DSS06.02, DSS06.03, APO01.06, DSS01.01, DSS05.02, DSS05.06, DSS06.04, dan DSS06.05. Kemudian diidentifikasi 22 key risk indicator yang berhubungan dengan IT goal and 47 yang terpengaruh process goal. Dua komponen kontrol risiko tersebut yaitu enabler proses dan key risk indicator kemudian digunakan sebagai kontrol pada pengembangan 7 disain mitigasi risiko OSD PSE. Akhirnya penelitian ini menghasilkan rancangan pengembangan disain mitigasi risiko terhadap: Penyalahgunaan hak akses, kesalahan proses verifikasi sertifikat elektronik, kegagalan proses instalasi dan konfigurasi sistem, penyadapan, private key compromise, perangkat tidak dapat diakses dan adanya bug pada sistem OSD PSE.

<hr>

ABSTRACT

</p><hr /><p>Secara Elektronik (OSD PSE), is provided by a unit at National Cyber and Crypto Agency. This is an in-demand service for many sectors that require secure electronic procurement. This study focused on the identification, analysis and risk response of OSD PSE services to obtain an enabler process and key risk indicator by combining the Risk Scenario Risk Scenario COBIT 5 method and NIST SP 800-30 Revision 1. Based on the results of the study obtained 14 enabler processes that were successfully identified, namely APO07.01, APO07.03, APO07.06, DSS01.01, DSS01.04, DSS05.05, DSS06.02, DSS06.03, APO01.06, DSS01.01, DSS05.02, DSS05.06, DSS06.04, dan DSS06.05. Then 22 key risk indicator related to IT goal and 47 influenced by the process goal. These two components of risk control are then used as controls in the development of 7 OSD PSE risk mitigation design. Finally, this research produced a draft of the development of risk mitigation designs for: Access rights from prior roles are abused, error in the electronic certificate verification process, failure of the installation and system configuration process, private key compromise, hardware components inaccessible, and immature software (bugs) on the OSD PSE system.</p></i>