

Kerangka Kerja Socioteknikal Pengamanan Infrastruktur Informasi Vital Sektor Administrasi Pemerintahan di Indonesia = Sociotechnical Framework for Securing Vital Information Infrastructure in the Government Administration Sector in Indonesia

Prasetyo Adi Wibowo Putro, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920551939&lokasi=lokal>

Abstrak

Secara umum, kebijakan pengamanan infrastruktur informasi vital (IIV) di Indonesia mengacu pada undang-undang informasi dan transaksi elektronik, undang-undang keterbukaan informasi publik, undang-undang Pelindungan data pribadi dan peraturan Pelindungan IIV. Berdasarkan peraturan Pelindungan IIV, program pengamanan IIV setidaknya membutuhkan kerangka kerja pengamanan layanan IIV dan metode identifikasi layanan vital sesuai model pengamanan IIV. Dalam rangka memberikan panduan praktis serta memenuhi kebutuhan strategis, diusulkan rancangan kerangka kerja pengamanan IIV sesuai kebutuhan di Indonesia. Memperhatikan keterbatasan waktu penelitian, rancangan kerangka kerja dibangun mengacu kepada kebutuhan sektor administrasi pemerintahan sebagai sektor yang banyak terhubung dengan sektor strategis lain.

Penelitian kerangka kerja pengamanan IIV sektor administrasi pemerintahan dilakukan dengan pendekatan sosioteknikal mengacu metode predicting malfunctions in socio-technical systems (PreMiSTS). pada akhir penelitian dibuat sistem pendukung keputusan sebagai implementasi dari kerangka kerja yang dihasilkan. Keseluruhan tahapan penelitian didesain sebagai penelitian mixed method dengan kombinasi metode analisis data tematik, fuzzy delhphi method (FDM), partial least squares structural equation model (PLS SEM), teori desain visual, focus group discussion (FGD), dan content validity indeks (CVI).

Kerangka kerja yang dihasilkan memiliki 6 elemen penentu pengamanan IIV dengan total 20 sub elemen dan 36 indikator. Berdasarkan hasil FDM dan PLS SEM, semua elemen dan sub elemen berpengaruh, namun ada 5 indikator yang harus dihilangkan karena tidak berpengaruh. Berdasarkan nilai CVI, desain kerangka kerja dinyatakan oleh 7 narasumber memenuhi 7 kriteria kerangka kerja, yaitu simplicity, coverage, compliance, dynamics, capabilities, usefulness, dan trustworthiness. Implementasi kerangka kerja dalam bentuk sistem pendukung keputusan memberikan rekomendasi kendali pengamanan untuk setiap fungsi. Kebermanfaatan ini dapat diterima dengan Baik oleh responden

Penelitian ini memberikan kerangka kerja praktis untuk melindungi IIV di sektor pemerintahan Indonesia. Secara teoritis, penelitian ini memberikan kontribusi dalam identifikasi elemen keamanan dengan pendekatan sosioteknikal, serta metode validasi dan evaluasi kerangka kerja di bidang keamanan siber.

.....In general, the policy for securing critical information infrastructure (CII) in Indonesia refers to the information and electronic transactions law, the public information disclosure law, the personal data protection law and the CII protection regulations. Based on the CII Protection regulations, the CII security program requires at least an CII service security framework and vital service identification methods according to the CII security model. In order to provide practical guidance and meet strategic needs, a draft CII security framework is proposed according to needs in Indonesia. Taking into account the limited research time, the framework design was built referring to the needs of the government administration sector

as a sector that is widely connected with other strategic sectors.

Research on the CII protection framework for the government administration sector was carried out using a sociotechnical approach referring to the predicting malfunctions in socio-technical systems (PreMiSTS) method. At the end of the research a decision support system was created as an implementation of the resulting framework. The entire research stage was designed as mixed method research with a combination of thematic data analysis methods, fuzzy Delphi method (FDM), partial least squares structural equation model (PLS SEM), visual design theory, focus group discussion (FGD), and content validity index (CVI). The resulting framework has 6 elements determining IIV security with a total of 20 sub-elements and 36 indicators. Based on the results of FDM and PLS SEM, all elements and sub-elements have an influence, but there are 5 indicators that must be removed because they have no effect. Based on the CVI scores, the framework design was stated by 7 sources as meeting 7 framework criteria, namely simplicity, coverage, compliance, dynamics, capabilities, usefulness and trustworthiness. Implementation of the framework in the form of a decision support system provides security control recommendations for each function. This usefulness was well received by respondents

This research provides a practical framework for protecting CII in the Indonesian government sector. Theoretically, this research contributes to the identification of security elements using a sociotechnical approach, as well as validation and evaluation methods for frameworks in the field of cyber security.