

Perancangan Kebijakan Keamanan Informasi: Studi Kasus Instansi XYZ = Designing Information security policies, Case study: XYZ Institute

Thea Nisaa Andi Saffanah, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920519354&lokasi=lokal>

Abstrak

Pada bulan September 2021, dilaporkan adanya dugaan pembobolan dan penyusupan hacker kedalam 10 Kementerian, Lembaga dan Instansi Pemerintah. Instansi XYZ adalah salah satunya. Instansi XYZ merupakan badan pengawas pemerintah yang belum menerapkan dan merancang kebijakan keamanan informasi dengan baik. Adanya peraturan dari Kementerian Kominfo dan BSSN terkait dengan keamanan informasi, membuat Instansi XYZ berinisiatif untuk memperbaiki kebijakan keamanan informasi sesuai dengan standar yang ditentukan oleh Kementerian Kominfo dan BSSN, yakni dengan menggunakan standar SNI ISO/IEC 27001:2013 Kebijakan keamanan informasi di Instansi XYZ dirancang sebagai acuan dalam mengidentifikasi dan memahami penilaian aset, ancaman, kerentanan, kemungkinan terjadinya gangguan, dan dampak yang didapatkan terhadap keamanan informasi. Penelitian ini dibuat dengan tujuan untuk merancang kebijakan keamanan informasi di Instansi XYZ menggunakan standar SNI ISO/IEC 27001:2013. Pengumpulan data dan uji validasi rancangan kebijakan keamanan informasi dilakukan dengan menggunakan metode wawancara dengan pihak terkait, antara lain: Kepala TI, sub koordinator keamanan informasi TI sub koordinator informasi, sub koordinator tata kelola TI dan manajemen risiko TI, dan sub koordinator infrastruktur. Selain itu, pengumpulan data juga dilakukan dengan melakukan analisis dokumen internal organisasi, studi literatur, dan mengkaji penelitian-penelitian yang dilakukan sebelumnya. Adapun penelitian ini dilakukan dengan beberapa tahapan, yaitu identifikasi aset, ancaman dan kerentanan; identifikasi risiko; penilaian risiko; penentuan kontrol risiko. Hasil penelitian ini memberikan rancangan kebijakan keamanan informasi yang sesuai dengan Instansi XYZ.

.....In September 2021, it was reported that there were allegations of hacking and cyber-attack on 10 ministries, institutions, and government in Indonesia. XYZ Institute is one of them. XYZ Institute is a government supervisory that has not implemented and designed information security policies properly. Following regulations from the Ministry of Communications and Informatics and BSSN related to information security, made XYZ Institute take the initiative to improve information security policies in accordance with the standards set by the Ministry of Communications and Informatics and BSSN using SNI ISO/IEC 27001:2013 The information security policy at XYZ Institute is designed as a reference in identifying and understanding the assessment of assets, threats, vulnerabilities, the possibility of interference, and the impact on information security. This study aims to design an information security policy at XYZ Institute, using the SNI ISO/IEC 27001:2013 as the standard. The data collection and validation test of the information security policy design was created by interviewing related parties, including head of IT, IT information security sub-coordinator, information sub-coordinator, IT governance and IT risk management sub-coordinator, and infrastructure sub-coordinator. In addition, data collection was performed by analyzing the organization's internal documents, literature studies and reviewing previous studies. The stages carried out in this research are the identification of assets, threats, and vulnerabilities; risk identification; risk assessment; risk control determination. The results of this study provide an

information security policy design that is in accordance with XYZ Institute.