Perancangan Kerangka Kerja Manajemen Insiden Keamanan Informasi Menggunakan Standar ISO/IEC 27035 Pada Layanan Data Dan Informasi Di Instansi XYZ = Design of an Information Security Incident Management Framework Based on Risk Analysis Using ISO/IEC 27035 Standards on Data and Information Services at XYZ Agencies

Ignatius Frank Zinatra Poetiray, author

Abstrak

Proses pengelolaan data dan informasi di Instansi XYZ memiliki ancaman risiko insiden keamanan informasi dan belum fokus terhadap aspek penanganan insiden keamanan informasi. Hal ini dikarenakan pemetaan ancaman, dampak dan potensi risiko insiden keamanan informasi yang ada di Instansi XYZ belum memadai dan belum tersedianya strategi dalam meningkatkan manajemen insiden keamanan informasi agar dapat membantu Instansi XYZ dalam menghadapi ancaman insiden keamanan informasi dan menjamin keamanan pelayanan data informasi instansi kepada masyarakat. Pengumpulan data dilakukan melalui wawancara dengan pejabat dilingkungan Instansi XYZ dan hasil analisis risiko didapatkan jumlah total 271 risiko yang dimiliki Instansi XYZ, dengan jumlah risiko inheren terdapat 4 risiko dengan level tinggi, 184 risiko dengan level sedang dan 79 risiko dengan level rendah. Dalam melakukan penyusunan rekomendasi, digunakan pendekatan kesesuaian dari insiden manajemen keamanan informasi menurut SNI ISO/IEC 27035 dengan proses bisnis. Penelitian menghasilkan bahan evaluasi dan rekomendasi dalam aspek kerangka kerja yang digunakan bagi peningkatan kinerja Instansi XYZ dalam penanganan ancaman insiden keamanan informasi.

.....The process of managing data and information at the XYZ Agency has a risk of information security incidents and has not focused on aspects of handling information security incidents. This is due to the inadequate mapping of threats, impacts and potential risks of information security incidents at the XYZ Agency and the unavailability of strategies to improve information security incident management so that they can assist XYZ Agencies in dealing with the threat of information security incidents and guarantee the security of agency information data services to the public. Data collection was carried out through interviews with officials within the XYZ Agency and the results of the risk analysis obtained a total of 271 risks owned by the XYZ Agency, with the total inherent risk being 4 risks with a high level, 184 risks with a moderate level and 79 risks with a low level. In preparing the recommendations, the conformity approach of information security incident management according to SNI ISO/IEC 27035 with business processes is used. The research produced evaluation materials and recommendations in terms of the framework used to improve the performance of the XYZ Agency in handling information security incident threats.