Usulan metrik untuk mengukur level pengamanan informasi berbasis ISO 27001:2005 (Studi Kasus Tim SKTI-DTI Bank X)

Arian Dhini, author

Abstrak

Pengamanan informasi merupakan isu yang semakin penting akhir-akhir ini. Mengingat informasi merupakan aset yang paling berharga bagi sebuah organisasi, sedangkan ancaman untuk mengganggu informasi yang semakin meningkat. Untuk itu diperlukan implementasi Information Security Management System (ISMS) dalam lingkungan organisasi untuk menjaga informasi, sehingga confidentiality, integrity dan availabilitiy informasi selalu terjaga. ISO/IEC 27001:2005 merupakan standar internasional pengamanan informasi yang menggunakan pendekatan perbaikan yang kontinyu. Tim SKTI - DTI Bank X di akhir 2006 lalu berhasil mendapatkan sertifikasi ISO 27001.
Dalam upaya mempertahankan sertifikat ISO 27001 dan terutama meningkatkan implementasi ISMS di lingkungan organisasi tersebut, pengukuran pengamanan informasi merupakan salah satu metode untuk memantau pengamanan informasi yang dijalankan. Untuk itu, dalam penelitian ini diusulkan metrik pengamanan informasi (18), sebagai pelengkap metrik pengamanan informasi yang sudah dimiliki (12). Metrik pengamanan informasi tersebut terdiri dari 4 klasifikasi, yaitu kontrol manajemen, proses bisnis, kontrol operasional dan kontrol teknis. Selanjutnya dilakukan pengukuran menggunakan metrik yang diusulkan dan yang terpasang, di mana data-data berasal dari data historis, dokumentasi bukti implementasi,hasil kuesioner dan wawancara. Hasil pengukuran tersebut ditampilkan dalam bentuk tabel dan grafik, sehingga bisa memberikan gambaran tentang level pengamanan informasi di lingkungan Tim SKTI tersebut, berdasarkan kriteria pengamanan informasi yang diukur.
.....Information security becomes important topics nowadays. Since information is the most valuable asset in any organization and threats to information have been always increasing, the information-based organization needs to keep Information Security Management System (ISMS) which aims to preserve the confidentiality, integrity and availability of information. ISO/IEC 27001: 2005 is international standard in information security using a continual improvement approach. The IT Directorate's SKTI Team in Bank X received the certification of ISO 27001 in the end of 2006.
In order to maintain the ISO 27001 certified's predicate and to improve ISMS implementation, the organization needs to measure information security as a way to monitor the information security activities. This research proposes 18 new information security metrics to compliment the existing twelve IS metrics. These IS metrics consist of four classifications, i.e. management control, business process, operational control, and technical control. The discussion covers the conducts of information security measurement using both existing and proposed IS metrics. These measurements processed data sourced from historical data, the records of implementation evidences, questionnaires, and interviews. The results of the information security criteria based measurements are represented in the form of both tables and graphs to gauge the implementation level of information security in the SKTI Team.