Instrumen Penilaian Sistem Manajemen Keamanan Informasi dengan Integrasi Standar ISO 27002 dan ISO 27004 = Assessment Instrument for Information Security Management System with Integration of ISO 27002 and ISO 27004 Frameworks

Khafidh Sunny Al Fajri, author

Abstrak

Pertumbuhan pesat teknologi informasi dan komunikasi juga mengakibatkan peningkatan signifikan tindakan kejahatan siber. Menurut Laporan Pemantauan Keamanan Siber Tahunan oleh Badan Siber dan Sandi Negara, terjadi 495 juta kejadian anomali lalu lintas atau upaya serangan pada tahun 2020, yang meningkat menjadi 1,6 miliar pada tahun 2021 di Indonesia. Penerapan standar ISO 27001 untuk sistem manajemen keamanan informasi (SMKI) dapat membantu mengurangi upaya serangan siber tersebut. Penelitian ini berfokus pada studi kasus lembaga pemerintah, Direktorat Informasi Kepabeanan dan Cukai, yang beroperasi di bidang penerimaan bea dan cukai dan telah menerapkan SMKI serta menjalani audit internal, namun hanya sebatas kelengkapan dokumen saja. Oleh karena itu, diperlukan pemodelan penilaian SMKI yang lebih mendalam sesuai dengan standar ISO 27001. Penelitian ini mengusulkan model penilaian SMKI dengan mengintegrasikan ISO 27002 dan 27004, dimana fungsi panduan ISO 27002 diubah menjadi parameter penilaian dan ISO 27004 digunakan untuk mengukur kinerja kontrol keamanan informasi. Dengan menggunakan model ini, nilai SMKI dari studi kasus diperoleh sebesar 45,17 dari skala 100 yang jauh berbeda dengan hasil audit internal studi kasus bernilai 4,08 dari skala 5 atau 82 dari skala 100. .....The rapid growth of information and communication technology has led to a significant increase in cybercrime. According to the Annual Cybersecurity Monitoring Report by the National Cyber and Cryptography Agency, there were 495 million instances of traffic anomalies or attempted attacks in 2020, which rose to 1.6 billion in 2021 in Indonesia. The implementation of the ISO 27001 standard for Information Security Management Systems (ISMS) can help mitigate these cyberattack efforts. This research focuses on a case study of a government institution, the Directorate of Customs and Excise Information, operating in customs duty collection, which has implemented ISMS and undergone internal audits, but only to the extent of document completeness. Therefore, a more in-depth ISMS assessment model is needed in accordance with ISO 27001 standards. This study proposes an ISMS assessment model by integrating ISO 27002 and 27004, wherein the functions of ISO 27002 guidelines are transformed into assessment parameters, and ISO 27004 is utilized to measure the performance of information security controls. Using this model, the ISMS score for the case study is determined to be 45.17 on a scale of 100, which significantly differs from the internal audit results of the case study, valued at 4.08 on a scale of 5 or 82 on a scale of 100.