Audit kepatuhan keamanan informasi dengan menggunakan kerangka kerja iso/iec 27001: studi kasus PT XYZ = Compliance audit of information security using iso/iec 27001 framework: PT. XYZ case study

Taofik Haryanto, author

Abstrak

Pengelolaan informasi yang baik dapat menjaga keberlanjutan bisnis perusahaan, memanfaatkan peluang bisnis, dan memaksimalkan nilai return dari investasi. Pengelolaan keamanan informasi dilakukan perusahaan dengan membuat Sistem Manajemen Keamanan Informasi (SMKI) untuk mengantisipasi setiap ancaman terhadap aset informasi. Standar SMKI yang banyak diadopsi adalah ISO/IEC 27001:2005. Standar versi 2005 ini mengalami revisi pada tahun 2013. Dengan adanya revisi tersebut, maka perusahaan yang telah memiliki sertifikasi ISO/IEC 27001 harus melakukan penyesuaian SMKI agar tetap selaras dengan versi 2013.
PT. XYZ sebagai operator selular dengan jumlah pelanggan terbanyak di Indonesia mengelola aset informasinya dengan menerapkan SMKI berbasis ISO/IEC 27001:2005. PT. XYZ harus menyesuaikan SMKI dengan versi 2013 agar pengelolaan keamanan informasi yang dilakukan tetap sesuai dengan best practices terbaru dalam mengatasi risiko informasi terkini. Penyesuaian ini juga menunjukkan komitmen PT. XYZ dalam melindungi data pelanggan, meningkatkan kredibilitas dalam pasar yang kompetitif, dan mempertahankan sertifikasi ISO/IEC 27001 yang pernah diraihnya. Untuk itu perlu dilakukan audit kepatuhan keamanan informasi yang berlaku di PT. XYZ terhadap ISO/IEC 27001:2013. Penelitian menunjukkan sejauh mana SMKI PT. XYZ patuh terhadap ISO/IEC 27001:2013. Untuk meningkatkan kepatuhan direkomendasikan beberapa kebijakan dan prosedur yang perlu ditambahkan, yaitu terkait komunikasi SMKI kepada pihak terkait, kontrol terhadap supply chain, dan kontrol redundan.
.....Information management will maintain the sustainability of the company's business, take advantage of business opportunities, and maximize the return value of the investment. Information Security Management System (ISMS) done by enterprise to anticipate any threats to information assets. Widely adopted ISMS standard is ISO / IEC 27001: 2005. This version of the standard was revised in 2013. With this revision, the company with ISO / IEC 27001 Certification should make adjustments to comply with new standard.
PT. XYZ as a service provider with the highest number of subscribers in Indonesia manage their information assets by implementing ISMS based on ISO / IEC 27001:2005. PT. XYZ must adjust the ISMS in order to stay aligned with the latest best practices and newest information risk. This adjustment also shows the commitment of PT. XYZ in protecting customer data, improving credibility in a competitive market, and maintain ISO / IEC 27001 Certification. Therefore, compliance audit of information security in PT. XYZ need to be done. Audit shows the extent of the ISMS adherence to ISO / IEC 27001:2013. To improve compliance, we recommend several policies and procedures that need to be added: communications to related parties, control of the supply chain, and control of redundancy.