Evaluasi Dan Penilaian Risiko Keamanan Informasi Menggunakan ISO/IEC 27001: Studi Kasus PT XYZ = Information Security Evaluation And Risk Assessment Using ISO/IEC 27001: Case Study of PT XYZ

Dayyan Fatih, author

Abstrak

PT XYZ merupakan salah satu Badan Usaha Milik Pemerintah (BUMN) Republik Indonesia yang bergerak pada bidang agribisnis. PT XYZ sudah memiliki sistem manajemen keamanan informasi (SMKI), namun masih ditemukan beberapa kendala seperti atensi personil terhadap keamanan informasi yang rendah, kebutuhan untuk tetap patuh dengan peraturan pemerintah, hingga kendala teknis yang muncul, sehingga PT XYZ ingin meningkatkan kapabilitas terkait keamanan informasi yang mereka miliki. Penelitian ini bertujuan untuk mengetahui kondisi terkini dari SMKI yang ada pada PT XYZ dan memberikan rekomendasi peningkatan SMKI. Penelitian ini menggunakan kontrol keamanan informasi berdasarkan standar ISO/IEC 27001:2022 untuk mendapatkan gap kondisi keamanan informasi, dan kemudian melakukan penilaian risiko yang memakai data hasil gap yaitu kontrol keamanan informasi yang terpilih. Setelah itu dilakukan rekomendasi yang disusun berdasarkan standar ISO/IEC 27002:2022. Temuan dari penelitian ini adalah ditemukannya 22 aktivitas kontrol ISO/IEC 27001:2022 yang hasil nilainya belum maksimal. 22 kontrol ini kemudian dibagi menjadi 3 kategori rekomendasi berdasarkan urgensi peningkatan yang sesuai dari hasil penilaian risiko.

..... PT XYZ is one of the government-owned enterprises of the Republic of Indonesia that engaged in agribusiness. PT XYZ already has an information security management system (ISMS), but there are still several obstacles that are found, such as low personnel attention to information security, the need to remain compliant with government regulations, to technical constraints that arise, so PT XYZ wants to improve its information security-related capabilities. This study aims to determine the current condition of the existing ISMS at PT XYZ and provide recommendations for improving the ISMS. This research uses information security controls based on the ISO/IEC 27001: 2022 standard to get the information security condition gap, and then conduct a risk assessment using the gap result data, namely the selected information security controls. After that, recommendations were made based on the ISO / IEC 27002: 2022 standard. The findings of this study were the discovery of 22 ISO/IEC 27001:2022 control activities whose value results were not maximised. These 22 controls are then divided into 3 categories of recommendations based on the urgency, from the results of the risk assessment.