Audit kepatuhan keamanan informasi dengan menggunakan framework ISO 27001/ISMS: Studi kasus PT XYZ = Information security compliance audit with ISO 27001/ISMS framework: Case study PT XYZ

Dzikril Hakim Nur Hisyam, author

Abstrak

Perkembangan teknologi informasi mempunyai risiko yang cukup signifikan terhadap suatu perusahaan. Selain dapat mempermudah dan mempercepat proses bisnis tetapi juga dapat membawa risiko dan ancaman terhadap perusahaan. Untuk itu diperlukan kontrol yang dapat memitigasi atau bahkan dapat menghilangkan risiko yang ada, sehingga teknologi informasi yang diterapkan organisasi dapat mendukung sepenuhnya kepentingan organisasi. Hal ini bertujuan agar teknologi informasi memberikan manfaat bagi organisasi. Kondisi saat ini PT. XYZ telah melakukan berbagai usaha untuk dapat memitigasi atau bahkan menghilangkan risiko keamanan informasi yang ada, tetapi karena belum adanya kerangka kerja yang digunakan sehingga sulit bagi PT. XYZ untuk mengukur dan menjalankan keamanan informasi secara optimal.

Mengacu pada kondisi dan permasalahan di organisasi tersebut, maka perlu adanya evaluasi keamanan informasi untuk mengukur sejauh apa usaha PT. XYZ telah menerapkan keamanan informasi dan kontrol-kontrol apa yang perlu ditambahkan atau diperbaiki agar usaha PT. XYZ dalam menerapkan keamanan informasi menjadi optimal.

Pada penelitian ini menggunakan Framework ISO 27001:2005/ISMS. Melalui pendekatan audit keamanan informasi dengan menggunakan assessment checklist ISO 27001 dan penilaian risiko, dipilih sasaran perbaikan berdasarkan kontrol ISO 27001. Kontrol-kontrol ini nantinya diharapkan dapat memitigasi atau bahkan menghilangkan dampak yang ditimbulkan dari ancaman dan kerawanan yang ada dilingkungan organisasi PT. XYZ.

.....The development of information technology has a significant risk of a company. Besides being able to simplify and speed up business processes but can also bring risks and threats to the company. It is necessary to control that can mitigate or even eliminate existing risks, so that the applied information technology organizations can support fully the interests of the organization. It aims to provide the benefits of information technology to the organization.

Current conditions PT. XYZ has made various efforts to mitigate or even eliminate the risk of information security, but because of the absence of a framework used so difficult for PT. XYZ to measure and run an optimal information security.

Referring to the conditions and problems in the organization, hence the need for information security evaluation to measure the extent to which PT. XYZ has implemented information security and controls what needs to be added or improved in order PT. XYZ in implementing information security to be optimal.

In this study, using the Framework ISO 27001: 2005 / ISMS. Through approach to information security audit using a checklist ISO 27001 assessment and risk assessment, have been targets for improvement based on the control of ISO 27001. These controls might be expected to mitigate or even eliminate the impact of threats and vulnerabilities that exist within the organization PT. XYZ.