Evaluasi dan Rekomendasi Manajemen Risiko Keamanan Informasi: Studi Kasus PT XYZ = Evaluation and Recommendations of Information Security Risk Management: A Case Study of PT XYZ

Anggoro Gagah Nugroho, author

Abstrak

Organisasi perlu menerapkan suatu keamanan informasi yang baik agar proses bisnis organisasi bisa berjalan tanpa ada ancaman. Aset TI merupakan hal yang harus dilindungi dikarenakan berpengaruh dengan proses bisnis organisasi. PT XYZ bergerak dibidang manage service untuk network dan juga cloud. Apabila terjadi kendala pada operasional organisasi dapat mengganggu Service Level Agreement (SLA) dengan pelanggan dan proses bisnis internal. Oleh karena itu, dibutuhkan manajemen risiko keamanan informasi yang tepat dan akurat. Permasalahan pada PT XYZ tidak pernah melakukan pembaharuan terhadap manajemen risiko sudah lebih dari tiga tahun, yang mana organisasi belum mengetahui jika terdapat risiko baru yang mengancam operasional. Operation risk atau risiko operasional akan diteliti dikarenakan operation risk akan berdampak kepada SLA pelanggan dan juga proses bisnis PT XYZ. Sudah ada dua kejadian serangan yang terjadi seperti DDOS Attack dan Ransomware pada aset organisasi beberapa waktu lalu. Maka dari itu dalam suatu organisasi diharuskan mempunyai manajemen keamanan informasi untuk dapat mengontrol segala risiko yang ada agar tidak menimbulkan kerugian pada organisasi. Untuk kerangka kerja dari keamanan informasi menggunakan kontrol dari ISO/IEC 27001:2013 sebagai acuannya. Tujuan dari penelitian ini adalah memberikan rekomendasi usulan ruang untuk berkembang pada organisasi khususnya pada operation risk PT XYZ. Dengan hasil evaluasi kondisi manajemen risiko keamanan informasi menggunakan standar ISO/IEC 27001:2013, didapatkan analisis kesenjangan dengan keamanan informasi pada organisasi sebesar 83,91% atau sebagian besar tercapai. Selanjutnya untuk rekomendasi ruang untuk berkembang menggunakan 10 rekomendasi kontrol dalam bentuk Statement of Applicability (SOA) dan usulan 10 pemilihan kontrol risiko pada risiko yang masih berstatus mitigasi pada operation risk. .....Organizations must be able to implement a good information security so that the organization can run its business processes without any threats. IT assets are things that must be protected because they affect the organization's business processes. PT XYZ is engaged in managing services for the network and the cloud services. If there are operational problems, the organization cannot monitor links that are down, it will disrupt the Service Level Agreement (SLA) with user and internal business processes. Therefore, appropriate and accurate information security risk management is needed. The problem is that PT XYZ has never updated its risk management for more than three years, which is where the organization does not know if there are new risks that threaten operations. Operation risk or operational risk will be investigated because operation risk has an impact on pelanggan SLA and also organization’s business processes. There have been two incidents of attacks such as DDOS Attack and Ransomware on organizational assets some time ago. Therefore, an organization is required to have information security management to be able to control all existing risks so as not to cause harm to the organization. For the framework of information security using the objective control of ISO/IEC 27001:2013 as a reference. The purpose of this study is to provide recommendations for space proposals to develop in the organization, especially in the operation risk of PT XYZ. With the results of the evaluation of the condition of information security risk management

using the ISO/IEC 27001:2013 standard, it was found that a gap analysis with information security in the organization was 83.91% or most of it was achieved. Then for recommendations for space to develop, use 10 objective controls in the form of a Statement of Applicability (SOA) and a proposed 10 selection of risk controls on risks that are still in the status of mitigation on operation risk.