Recommendations for Information Security and Risk Management

Table of Contents

Introduction

Considering the assessment of risks being identified within an organization, the paper is illustrating the recommendation and explanation for implementing the practices in support of information security and risk management.

Suggestions for Information Security and Risk Management

An organization is suggested to apply the recent clauses of ISO/IEC for information security management systems to support the business and risk oriented approach. The requirements of businesses regarding information security are required to be identified by a methodical assessment of security risks. Management of an organization is required to specify its approach so that the business can be managed within the same context (Balzacq, 2011). It should be noted that an organization should specify risk assessment as an activity that is required to be approached within the context of an organization's broader enterprise risk management framework. The international codes of practice for information technology provide a specification that sets out the requirements for an information security management system (Ballad, Ballad, & Banks, 2010).

The standard ~~codes provide~~ a practical solution to the wide range of regulatory requirements related to information technology as well as help an organization to more cost effectively counter the increasing range of information security threats. The personnel security metrics are required to quantify the percentage of users with special access to systems having background evaluations (Alpcan & Başar, 2010). The security awareness metrics are concerned with the percentage of employees with significant security responsibilities. The data integrity metrics are also required to be enforced because they quantify the percentage of systems with

automatic virus definition updates along with automatic virus scanning and the percentage of systems performing password policy verification. There should be contingency planning measurements including the percentage level of critical data files and operations with established backup and contingency plan (Balzacq, 2011).

Conclusion

It can be concluded that the execution of strategies to prevent the information security and risk management in an organization requires an organization to implement certain metrics while considering the risks being analyzed and assessed.

Reference

Alpcan, T., & Başar, T. (2010). *Network Security: A Decision and Game-Theoretic Approach.* New Delhi: Cambridge University Press.

Ballad, B., Ballad, T., & Banks, E. (2010). *Access Control, Authentication, and Public Key Infrastructure.* Jones & Bartlett Publishers.

Balzacq, T. (2011). *Securitization Theory.* New York: Taylor & Francis.