An Overview of the IT Risk Management Methodologies for Securing Information Assets

Sayan Mercan Dursun
Fortinet, USA

Meltem Mutluturk
https://orcid.org/0000-0001-5666-594X
Bogazici University, Turkey

Nazim Taskin
Bogazici University, Turkey

Bilgin Metin
https://orcid.org/0000-0002-5828-9770
Bogazici University, Turkey

EXECUTIVE SUMMARY

Effective information asset management is the basis of information security as well as many other issues. IT risk assessments work well with the proper handling of asset values, and also it is for effectively securing information assets. There is also a wide variety of risk assessment methodologies. This chapter presents information about the overall IT risk management process and methodologies. Best practices are mentioned and occasionally compared based on the requirements of the information technology (IT) sector in practice. This chapter will provide deep knowledge about the IT risk management approach and construction to implementers, risk owners, IT auditors, executive managers, and other IT staff.

INTRODUCTION

Organizations are growing more aware of the role of information technology (IT) in managing knowledge

Copyright © 2022, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

through information systems (IS), which stores data that is used within an organization's business processes and value-adding operations (Wilkin & Chenhall, 2010). While the use of information technology (IT) within an organization acquires digitalization benefits, it also increases the attack surface for threat actors and brings about many risks. IT Risks such as an attack on the network infrastructure or data breaches are becoming more and more common. As companies become more dependent upon IT, the effects of loss of IT assets become critical. As IT is an important asset it must be managed accordingly to maximise the benefit while minimising the risks (Ernawati et al., 2012). Furthermore, organizations need to integrate the management of these risks with other processes; internal control, governance, operations, changes and other processes. Organizations are faced with a broad spectrum of enterprise risks that can affect their operations, and IT risk is one of these enterprise risks (Hopkin, 2018). IT risk can be defined as the likelihood of an event occurring based on a failure or misuse of IT that will impact an enterprise objective. An IT information security incident does not only affect a company's IT department or data centre; it may produce substantial business consequences that impact a wide range of stakeholders (Westerman & Hunter, 2007). The risk management process, although well defined, is presented in various approaches, frameworks, and standards. In order to understand the overall process of IT risk management and the different approaches taken in the literature, this study examines IT risk standards and frameworks and their methodologies. Firstly, the IT risk management process is defined. Subsequently, the standards and frameworks for IT risk management are examined. Lastly, the outcomes of conducting an IT risk management are given.

IT RISK MANAGEMENT PROCESS

Organizations intent on applying a risk management framework should first establish an IT Risk Management Team. This team should coordinate the risk management process and consult the organization throughout the process. Also, roles and responsibilities should be clearly defined. All participants should be assigned and informed to dedicate a serious period of time to the process. The basic IT risk management process can be found in Figure 1 below. Firstly, the risks of an organization should be defined and evaluated as to the impact the risks can have on the organization taking into account its risk tolerance. Then, the necessary controls that are already in place or should be in place to mitigate the defined risks need to be analysed in order to properly treat the risk which is the last step in the process. All the while, a continuous monitoring and reviewing process needs to be conducted in parallel.

Identify Risks

Risk is the probability of a threat exploiting a vulnerability that could potentially harm the organization's assets and business processes. Risk owners should define the threats and vulnerabilities of the individual risks. There are different approaches to identifying risks. It is observed that people coming from a more technical background define risks based on vulnerabilities as opposed to people with a background in business who define risks based on threats.

Risk owners are usually chosen from the technical department of an organization as they are more knowledgeable of the environment they work in, therefore, are more equipped to identify the possible risky areas. When defining risks, it is practical to create a list of the individual risks along with the vulnerability that gives rise to the risk and the asset that may be affected.

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/an-overview-of-the-it-risk-management-methodologies-for-securing-information-assets/289738

Related Content

Pseudo-Independent Models and Decision Theoretic Knowledge Discovery
Yang Xiang (2009). *Encyclopedia of Data Warehousing and Mining, Second Edition (pp. 1632-1638).*
www.irma-international.org/chapter/pseudo-independent-models-decision-theoretic/11037

Association Rule Mining of Relational Data
Anne Denton (2009). *Encyclopedia of Data Warehousing and Mining, Second Edition (pp. 87-93).*
www.irma-international.org/chapter/association-rule-mining-relational-data/10803

Association Rule Mining
Yew-Kwong Woon (2009). *Encyclopedia of Data Warehousing and Mining, Second Edition (pp. 76-82).*
www.irma-international.org/chapter/association-rule-mining/10801

Preservice Teachers Collaborating and Co-Constructing in a Digital Space: Using Participatory Literacy Practices to Teach Content and Pedagogy
Chrystine Mitchelland Carin Appleget (2020). *Participatory Literacy Practices for P-12 Classrooms in the Digital Age (pp. 215-232).*
www.irma-international.org/chapter/preservice-teachers-collaborating-and-co-constructing-in-a-digital-space/237423

Distributed Data Mining
Grigorios Tsoumakas (2009). *Encyclopedia of Data Warehousing and Mining, Second Edition (pp. 709-715).*
www.irma-international.org/chapter/distributed-data-mining/10898