Chapter 14
Information Security Risk Management in the European Union

Anca Gabriela Petrescu
Valahia University, Romania

Nicoleta Sirbu
Valahia University, Romania

ABSTRACT
Currently the organization’s risk management covers a wider range of risks, especially operational risks, reputation risks to the organization, and more recently, strategic risks. Moreover, within a growing number of organizations, responsibilities associated with risk management are assumed by the top management, which generally coordinates the teams of specialists directly responsible for monitoring the risks and the risk handling measures. This chapter focuses on how to implement an approach to reduce the identified risks to the information conveyed through computer systems and communications. In additional, it presents EU regulations relevant to the analysis and risk management information security.

INTRODUCTION
Risk management provides a clear and structured approach to identify organizational risks (Gandino, Celozzi & Rebaudengo, 2017; Stepchenko & Voronova, 2015). A clear understanding of the risks enables organizations to measure and prioritize them in order to be able to adopt the most appropriate measures to mitigate adverse

DOI: 10.4018/978-1-5225-7712-6.ch014
effects on the objectives set in addition, development of a risk management process has other benefits on organizations, such as: save resources: time, assets, income, property and personnel are valuable resources that can be properly managed if we take into account the results of risk analysis processes; protecting the reputation and public image of the organization; preventing or reducing legal issues and increased stability of the organization; protecting the population against various dangers; protecting the environment; increasing training capacity for different situations; clearly define insurance needs (Enagi & Ochoche, 2013).

An effective risk management does not eliminate the risk entirely (Andress, 2003). However, a practical and effective operational risk management demonstrates that the organization is making efforts to minimize or prevent losses, which brings benefits in terms of insurers (Barton, Tejay, Lane & Terrell, 2016).

On the other hand, there are organizations seeking maximize the benefits of modern technologies such as cloud computing, service oriented architectures, calling for it to external entities (Winkler, 2010). Given that the organization typically has no control over how external entity performing the analysis and handling of information security risks, additional risks may concerns the organization (Karim, 2007).

In addition to the impact of organizational culture on perspective approach to risk management within the organization, there may be cultural elements in the relationship between organizations (Fischbacher-Smith, 2016). When several organizations are working together to fulfill common objectives might appear different approaches that can lead to different risk management strategies, which would create new risks and determine the tendency to accept more readily the risks (Arukonda & Sinha, 2015).

The strategy of the risk acceptancy implies the loss acceptancy, if they appear (Collins & McCombie, 2012). This strategy is viable for low risk where measures to reduce the risk or insurance in case of injury are more costly in time than the potential loss (Hadžiosmanović, Bolzoni & Hartel, 2012). All risks that are not avoided or transferred should be reduced or accepted as such (Landoll, 2010). Also in this category includes risks that are so large or catastrophic that either cannot be made to cover their insurance or insurance premiums would be infeasible. An example is the war situation for the goods and risks are not insured. Risk can be accepted if the likelihood of major losses is very small or if the cost of insurance with higher coverage is very high and can cause problems in achieving the organization’s objectives (Eriksson & Kovalainen, 2015).

Most often, organizations adopt combined strategies for addressing the risks identified in the risk analysis stage security (Karanja, 2017). In dealing with risks to information conveyed through information and communication systems, the predominant strategy is to determine the implementation of measures to reduce risks so as to ensure the objectives of information security - confidentiality, integrity, availability, authenticity and non-repudiation - in order to fulfill properly the
Related Content

Winemaking Sector in Greece: An Accounting-Based Approach
[www.igi-global.com/article/winemaking-sector-in-greece/234334?camid=4v1a](www.igi-global.com/article/winemaking-sector-in-greece/234334?camid=4v1a)

Do Bankers Use Managerial Discretion with Regard to CSR and Earnings Management to Rebuild Their Reputation in the Aftermath of the Financial Crisis?
Convergence in Bank Credit: A Study of the Major Indian States over the Period 1972-2010
Ramesh Chandra Das and Soumyananda Dinda (2014). Global Strategies in Banking and Finance (pp. 101-120).
www.igi-global.com/chapter/convergence-in-bank-credit/94439?camid=4v1a

International Portfolio Diversification Benefits among Developed and Emerging Markets within the Context of the Recent Global Financial Crisis