Chapter 78
Risk and Security of Information Systems in the Portuguese Financial Sector: Model and Proof of Concept in Portuguese Regulator

Pedro Fernandes da Anunciação
Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal, Portugal

Alexandre Miguel Barão Rodrigues
Banco de Portugal, Portugal

ABSTRACT

This work follows the need of safety standards, update ISO27002:2013, in the major central banks of several European countries. This need has been studied by establishing a focus group that integrated European experts from major central banks. The analysis carried out was supported in the current methodology of information risk management, used by central banks in the safety management of information systems. This methodology is used to analyze and evaluate the adequacy of practices to risk management in the financial activity. The main objective was to present a proposal, sufficiently comprehensive and consistent, to a new risk management process of Information Systems within the European System of Central Banks. And a definition of a practical guide to risk management throughout the different stages of the Information Systems Life Cycle. The proposed model provides a higher degree of protection systems, technologies and information, especially in Central Banks, taking as reference the Portuguese Central Bank.

DOI: 10.4018/978-1-7998-7705-9.ch078

1. INTRODUCTION

Unlike other industries, the banking industry operates based on financial innovation, which greatly diversifies risk and creates profit through arbitrage (Wang & Lin, 2014). In the financial sector, managing operational risk is fetching an imperative piece of sound risk management practices in contemporary financial markets in the wake of a remarkable upsurge in the capacity of communications, high degree of structural changes and complex support systems. The most significant type of operational risk contains failures in internal controls and corporate governance (Baber, 2016). Formal corporate governance enhances shareholders' value (Yeh et al., 2014) and information technology governance (IT Governance) to financial institutions is a critical success factor to management internal controls. Financial institutions world-wide began to recognize operational risk in the 1990s. In that sense, the term operational risk is a recent phenomenon in the context of banking and financial institutions (Baber, 2016). The criticality of information technologies (IT) in the activities of financial institutions in general and banking in particular is directly related to the success or failure of business activities. We can understand failure as "Failure to Add Value" at every aspect of the Value Stream Cost (Total company wide cost of "Failure to Add Value". Using this comprehensive and inclusive definition, risk may be defined as the total company wide cost of "Failure to Add Value" per unit time (McLaughlin, 2015).

The IT Governance can be defined as the information technology management process in order to achieve the organizational objectives and create value through management and organizational control (ITGI, 2003). The IT Governance should provide a framework that makes easier the implementation of decisions required to manage, control and monitor IT with the business activities (Price Waterhouse Coopers, 2014).

Gartner conceptualizes the IT Governance in a more complete way, considering that IT Governance is defined as a process that ensure the effective and efficient use of IT in enabling organizations to achieve its goals. Information Systems (IS) are actually the backbone of economic organizations. So, it is important that top managers and IT managers understand the IT Governance as a process that can ensure, among others, some strategic benefits namely:

- The effectiveness of the IT investments (evaluation, selection, prioritization and viability);
- The management and oversee of the IT implementation; and
- The assessment of the business benefits.

IT Governance can also be approached in an operational perspective. In this case, IT Governance is concerned with the performance of IT and the evaluation of the effectiveness and efficiency of its support of the business activities. This is a responsibility of the Chief Information Officer.

Despite the relevance of IT Governance to the organizations, in general, and in the IT areas, in particular, there are some reasons that justify the difficulty in its adoption, namely:

- The lack of clear and formal responsibility for the IT areas, projects and services;
- The problems of communication between users of different organizational areas and IT suppliers;
- The gap between IT management and vision and business dynamics and objectives;
- The difficulties in value assessment and specification generated by IT to the business and organizational activities;
- The lack of metrics to evaluate the IT investments and its objectives;