Chapter 2

IT Governance Standards and Regulations

INTRODUCTION

Besides the economic aspect which affects the level of investment in IT infrastructure, from the standpoint of system availability, there are regulations that require some security controls in many industries. These regulations require investments in IT infrastructure even in cases when there is no economic justification but have a positive effect on raising the availability of IT systems.

For instance, IT systems in financial institutions are subject of regular audits by independent auditing companies which mostly rely on international standards for the management of IT systems. This is the indirect way of setting the requirements to align IT systems of financial institutions with these standards. It happens that the implementation of certain requirement of these standards has no economic justification, but its implementation reduces the risks of IS and increases system availability. An overview of some regulations and standards that banks must be in compliance with and that have direct impact on implementation of controls that improve system availability will be given in this chapter.

This chapter is composed of two parts: the first part presents the standards that are directly related to financial institutions and refer exclusively to them (Basel II and the payment card industry data security standard); second part considers standards for IS security management in general and can be applied on firms in all industries (ITIL, COBIT, ISO/IEC 27001:2013). Karkoskova

DOI: 10.4018/978-1-5225-2268-3.ch002
& Feuerlicht (2015) pointed out that ITIL and COBIT have similar objectives that include maximizing return on Investment, value creation, and IT investment optimization, leading to achievement of competitive advantage by using advanced IT technologies.

STANDARDS AND REGULATIONS FOR FINANCIAL INSTITUTIONS

Basel II

Basel II is a set of regulations adopted by the Basel Committee on Banking Supervision (hereinafter referred to as the Committee) which regulates the size of the bank’s capital relative to risk exposure. Basel II regulations are related to internationally active banks from the countries members of G10’s. The European Union has passed a directive (CAD3) that the provisions of the agreement became mandatory for all banks in the EU countries since the beginning of 2007.

According to the Basel II agreement, banks have to provide capital to cover expected losses on operational risk. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, systems or external events. This definition includes legal risk, but excludes strategic and reputational risk (Basel Committee on Banking Supervision, 2001). Security risks are a subset of operational risk. Figure 1 provides a classification of the loss event by type according to Basel II and BSI, which portrays that security risk are included in a large number of categories of operational risk.

Recognizing the specificity of electronic banking risk as well as its importance, the Committee issued a document “Risk Management Principles for Electronic Banking”, which deals with this issue. In this document, e-banking is defined as “the provision of retail and small value banking products and services through electronic channels as well as large value electronic payments and other wholesale banking services delivered electronically”. The document listed the following factors that may affect the risk management:

- The speed of change relating to technological and customer service innovation in e-banking is unprecedented. In order to efficiently maintain that pace, it is necessary for management to ensure adequate strategic assessment, risk analysis and security reviews are conducted prior to implementing new e-banking applications.
Innovation Efficiency and Open Innovation: An Application to Activity Branches in Spain
[www.igi-global.com/chapter/innovation-efficiency-open-innovation/60230?camid=4v1a](www.igi-global.com/chapter/innovation-efficiency-open-innovation/60230?camid=4v1a)

A Twofold Approach for Evaluating Inter-Organizational Workflow Modeling Formalisms
[www.igi-global.com/chapter/twofold-approach-evaluating-inter-organizational/6126?camid=4v1a](www.igi-global.com/chapter/twofold-approach-evaluating-inter-organizational/6126?camid=4v1a)