Risk Management Framework That Meets the Implementation Challenges in IT-Centric Micro and Small Companies

Jasmina Trajkovski, Trajkovski & Partners Management Consulting, Skopje, Macedonia
Ljupcho Antovski, Faculty of Computer Science and Engineering, University Ss. Cyril and Methodius, Skopje, Macedonia

ABSTRACT

This paper presents an overview of the proposed risk management framework and how it is designed to meet the challenges usually faced by IT-centric micro and small companies when implementing risk management. The issues and challenges identified for the IT-centric micro and small companies are centered around the exposure to various risks and necessity to have a risk management approach which covers these various risks, as well as to limited resources for risk management and necessity for usable and comprehensive framework. The new framework is based on the analysis of the best practices in risk management concepts as well as direct experience from dealing with over 20 companies in South-east Europe. The segments covered by the framework include people, policy, methodology and process, and tools.

Keywords: Enterprise Risk Management, International Organization for Standardization 27005 (ISO27005), International Organization for Standardization 31000 (ISO31000), IT-Centric Micro and Small Companies, Risk Management Framework, Risk Management Methodology

1. INTRODUCTION

In this paper we review the proposed risk management framework for IT-centric micro and small companies in our previous publication in light of the identified specifics and challenges faced by the IT-centric micro and small companies. The focus is on these specific companies is due to the direct experience of the leading author in the last 5 years with over 20 micro and small companies that are heavily IT-centric in their operations and the identified problems with the usage of other risk management frameworks. Solving this problem was the main driver for undertaking this PhD research.

The relevance of this paper for the IT Professionals is due to the ever growing importance of risk management in both strategic and daily...

DOI: 10.4018/jhcitp.2013040102
decision making of managers of any type of organization. Risk-based approaches are leading the way in various disciplines, such as internal auditing (Enescu & Maria, 2010), IT auditing (ISACA, 2009), software development project management (Sarigiannidis & Chatzoglou, 2011), information security (Corpuz & Barnes, 2010), aiming to focus the efforts and limited resources on the high priority and critical issues. The proposed risk management framework aims to address the issues and challenges of micro and small companies, mainly necessity to conduct risk management with limited resources and in a comprehensive but simple way. As the target users of the proposed methodology are IT-centric micro and small companies, the main risks to be covered by this methodology are operations risks, information security risks and IT risks.

This paper is structured in several segments. In Section 2, an overview of risk and risk management is provided together with introduction of the various types of risks and overview of risk management frameworks and standards. In Section 3, a short overview of the proposed Risk management framework is given. The specifics and challenges of IT-centric micro and small companies are presented in Section 4. Finally, in Section 5, a check is made to see how the proposed framework is addressing the issues relevant for the target group. The paper ends with conclusions and identifies further needed research.

2. OVERVIEW OF RISK AND RISK MANAGEMENT FRAMEWORKS AND STANDARDS

Gerber in the publication “Management of risk in the information age” (Gerber & von Solms, 2005) explains various aspects of risks and risk management. From the article, one can conclude that the main concepts of risks management can be divided into 2 groups: (i) definition of risk, types of risks and risk management, and (ii) risk management frameworks and standards.

Based on the International standard for Risk Management – ISO31000, risk is defined as: “effect of uncertainty on objectives” (ISO, 2009), where the uncertainties include events (which may or not happen) and uncertainties caused by ambiguity or a lack of information, while the objectives can have different aspects (health and safety, financial, IT, environmental) and can apply at different levels (such as strategic, organizational, project, process). It also includes both negative and positive impacts on objectives. The risk is often expresses as a combination of the consequences of an event and the associated likelihood of occurrence.

For the needs of the management of the IT-centric micro and small companies, all these risks could not be approached independently, and an integrated approach is necessary. This approach should be focused on the main drivers in the company, like the continual operations thru IT operation and known business processes so that the employees can understand what they should do. The reliance on IT as well puts the information security risks among the top as well. For the purposes of the research questions, we make the assumption that the management of these IT-centric micro and small companies deals with the legal and financial risks intuitively, and that they are not necessary to be included in the integrated risk management framework and approach of the company.

Having said that, for the purposes of the paper, we will look into the IT risk, information security risk and operational risk, which are respectively defined as:

- **IT Risk:** That is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. (ISACA, 2009)
Related Content

Organizational Learning and Collective Human Capital Relationship With Firm Performance Among MNEs in the Northern Region of Malaysia


Learning in Organizations: Some Observations from the Practice

[www.irma-international.org/article/learning-in-organizations/163410/](www.irma-international.org/article/learning-in-organizations/163410/)

A Study on Services Motivating Computing Professional Association Membership

[www.irma-international.org/article/study-services-motivating-computing-professional/63628/](www.irma-international.org/article/study-services-motivating-computing-professional/63628/)

Role Efficacy: Studying the Impact on Employee Engagement, Employee Motivation and Attrition

[www.irma-international.org/article/role-efficacy/121715/](www.irma-international.org/article/role-efficacy/121715/)

Organizational Advantages

[www.irma-international.org/chapter/organizational-advantages/31466/](www.irma-international.org/chapter/organizational-advantages/31466/)