Safety Science 89 (2016) 201–218

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

# An enhanced risk assessment framework for business continuity management systems

S. Ali Torabi [a,*], Ramin Giahi [a], Navid Sahebjamnia [b]

[a] School of Industrial Engineering, College of Engineering, University of Tehran, Tehran, Iran
[b] Department of Industrial Engineering, University of Science and Technology of Mazandaran, Behshahr, Iran

ARTICLE INFO

*Article history:*
Received 10 October 2015
Received in revised form 10 June 2016
Accepted 18 June 2016

*Keywords:*
Risk assessment
Business continuity management
Organizational resilience
Best-worst method
Resource allocation
Benefit-cost analysis

ABSTRACT

Every organization is exposed to several risks (e.g. cyber-attacks and disruptions caused by natural disasters). To respond to these risks properly, an effective risk management system should be implemented. Business continuity management is one of the most recent risk management frameworks, which enables the organizations to improve their resilience in order to cope with the identified risks. Risk assessment is one of the main parts of a business continuity management system (BCMS). In this paper, an enhanced risk assessment framework is proposed within the context of BCMS while accounting for specific steps and requirements of a BCMS. The proposed framework benefits from a suite of analytic techniques to enhance and facilitate the risk assessment and management within the well-known four-step framework (i.e. identifying, analyzing, evaluating, and responding to risks). The results of applying the proposed framework in a real case study demonstrate that it can effectively handle risk assessment and management process when implementing BCMS in an organization.



## 1. Introduction

The high rate of disruptive incidents, such as natural or technological ones, which take place around the world, encourages organizations to design and implement their own customized business continuity management system (BCMS) in order to get prepared for dealing with any possible disruption. Through implementing a BCMS, suitable business continuity plans (BCPs) are provided to respond to possible incidents (that could damage the organization's resources) in an efficient and effective way (Sahebjamnia et al., 2015). In this way, BCM could be viewed as a risk management system that enables organizations to improve their organizational resilience level.

According to (BS25999, 2007), the BCM life-cycle consists of six elements: BCM program management, understanding the organization, determining and identifying BCM strategies, developing and implementing BCM responses, embedding BCM in the organizational culture and also training, exercising, maintaining and reviewing the BCM plan. Understanding the organization is the key part of BCM. Business impact analysis (BIA) and risk assessment (RA) are two major tools of understanding the organization in the context of BCM (BS25999, 2007; Torabi et al., 2014). The purpose of BIA is to identify the critical functions needed to deliver key products/services, impact of disrupted activities on the organizations' objectives, and those resources needed to resume the critical activities after a crisis happens (BS25999, 2007). Also, RA is defined as the "overall process of risk identification, risk analysis and risk evaluation". The main objectives of RA in BCM are the identification of risks threatening the organization, their analysis and evaluation, and preparation for risk treatment and response planning ("ISO 22301," 2012).

The World Economic Forum's Global Risks 2015 report (Global Risks 2015, 10th Edition, 2015) states that risks threaten the human lives and organizations' activities. Organizations are exposed to a number of risks, which may disrupt their activities and cause lots of damages. For instance, a fire at a sub-supplier's plant caused $400 million losses for Ericsson in 2000 (Norrman and Jansson, 2004). Therefore, risks should be managed regularly to prevent losing resources and assets.

Owing to the fact that BCM is a kind of risk management it could be used as an appropriate tool to deal with risks. BCM is implemented to ensure delivery of the key products of organizations at any circumstances even after a risk occurs. However, BCM requires a comprehensive RA framework by which those risks threatening the organizations' activities could be identified, analyzed, evaluated, and responded. An appropriate RA framework helps organizations to make contingency plans to stop losing resources in the aftermath of a risk occurrence. In this paper, some

* Corresponding author.
*E-mail addresses:* satorabi@ut.ac.ir (S.A. Torabi), ramin.giahi@ut.ac.ir (R. Giahi), n.sahebjamnia@du.ac.ir (N. Sahebjamnia).

http://dx.doi.org/10.1016/j.ssci.2016.06.015
0925-7535/

analytical techniques are suggested to enhance and facilitate the risk assessment process within the BCMS context. For this, the literature of supply chain risks and organizational risks is first interrogated to find out the potential risks in service/manufacturing organizations. Then, risk factors (i.e. impact and likelihood of risks) are exploited by studying some relevant papers introducing risk factors. Thereupon, two effective methods are used to determine the impact and likelihood of risks (Feng et al., 2014; Halliday et al., 1996; Kangas and Kangas, 2004; Kull and Closs, 2008; Ritchie and Brindley, 2007; Samantra et al., 2014). Finally, after evaluating the risks, appropriate response plans are proposed to cope with them effectively. The main contributions of this paper can be outlined as follows:

- Conducting a comprehensive literature review to identify the most potential risks in the manufacturing and service organizations.
- Suggesting some analytical techniques to enhance and facilitate the risk assessment in the context of implementing the BCMS in an organization.
- Suggesting new sub-factors, which would help decision makers to measure the impact of risks more accurately.
- Proposing a new method to evaluate and respond to the identified risks.
- Developing a new method to provide needed resources to respond to a happened risk with regards to results of BIA and benefit/cost analysis.
- Applying the proposed framework and its suggested analytical tools in a real case study to handle the risk assessment and management process when implementing BCMS in a service organization.

In brief, the contributions of this paper are mainly related to proposing a suite of analytic techniques to improve while facilitate conducting the risk assessment and management process in the context of business continuity management systems within the well-known four-step framework of RA (see ISO 31010 for general overview of risk assessment & management). Noteworthy, this framework includes: (1) risk identification in which the potential risks of the organization are identified; (2) risk analysis in which the risk factors (i.e. risk likelihood and impact) are quantified and analyzed; (3) risk evaluation in which those risks needing treatment are determined; and finally (4) risk response planning in which the suitable response plans are developed.

The rest of the paper is organized as follows. Relevant literature is reviewed in Section 2. The suggested analytical tools for enhancing while facilitating the risk assessment process in the context of BCMS are elaborated in Section 3. In Section 4, applicability of the proposed framework and its analytical tools is demonstrated through conducting a real case study. Several managerial insights are derived from the numerical results in Section 5. Finally, Section 6 provides concluding remarks and directions for further research.

## 2. Literature review

Researchers have approached to RA in different ways. We group the literature review into the two main related areas including the supply chain and organizational RA.

### 2.1. RA in supply chains

RA is the main element of different risk management approaches (ISO 31010, 2009). Several works have been done to analyze, assess and manage supply chain risks (Hallikas et al., 2004; Kleindorfer and Saad, 2005; Lockamy, 2014). Hallikas et al. (2004) propose a risk management process for supply networks, which contains identification, assessment, treatment and monitoring risks. The paper states that risks are originated from: too low or inappropriate demand; problems in fulfilling customer needs; cost and prices; weakness in resources, development and flexibility. Kleindorfer and Saad (2005) propose a conceptual framework to manage disruption risks in supply chains. The paper categorizes the disruption risks as natural disasters, labor strikes, economic disruptions and terrorist attacks. Their proposed framework consists of three main steps including the identification of the sources of risks and vulnerabilities, risk assessment and mitigation. Wu et al. (2006) present a methodology to identify supplier-oriented risk factors and manage inbound supply risks. They classify the inbound risks according to their internal or external sources and controllability. Lockamy (2014) proposes a methodology to model and assess the suppliers' disaster risks in a supply chain network. After identifying the suppliers' risks, a Bayesian network is used to determine the risks' probabilities and the impact that a supplier could have on an organization using the Value-at-Risk (VAR) measure by which managers can decide whether continue with a supplier or not. The proposed methodology is also applied in an automotive company.

### 2.2. RA in organizations

There are some discrepancies with RA in manufacturing and service organizations (e.g. banking, tourism, hospitals and airports). In manufacturing and service organizations, risks are usually assessed by considering the delivery of products and services, respectively. It should be noted that although some parts of manufacturing organizations are comprised of service operations (e.g. customer relationship management and marketing operations), however, RA methods for manufacturing organizations cannot be used for all kinds of service organizations. In this section, the literature is reviewed in two separate but relevant streams, i.e., RA in manufacturing and service organizations.

#### 2.2.1. RA in manufacturing organizations

Although conducting RA in industrial firms is very important, many researchers have only focused on safety analysis and occupational risk assessment. Fera and Macchiaroli (2010) present a mixed qualitative-quantitative RA method for assessing the safety risks in the small and medium enterprises (SMEs). The authors introduce three steps for safety RA including the: (1) building a team to identify risks and comparing them with each other, (2) assessing them through a quantitative model to calculate the frequency and consequences of each identified risk and, (3) finally, providing improvement actions. Marhavilas and Koulouriotis (2012) present a framework for safety risk assessment in the work sites. In this framework, potential hazards are identified and their frequencies and consequences are analyzed using gathered relevant statistical data. After evaluating the hazards' quantities, suitable decisions about them are made (i.e. whether accept or mitigate each hazard).

There are several RA techniques which are often used in manufacturing organizations. Among them, failure mode and effect analysis (FMEA) (Chang and Cheng, 2010; Liu et al., 2015b; Song et al., 2014), fault tree analysis (FTA) (Lindhe et al., 2009; Liu et al., 2014), and hazards and operability study (HAZOP) (Trammell and Davis, 2001; Vinnem et al., 2006) are the most practical approaches. Table 1 shows a brief description on these methods.

Several models and frameworks have been proposed to conduct RA process in manufacturing organizations. Wulan and Petrovic (2012) present a framework for risk assessment within the context of enterprise collaboration. In this framework, different risks in the life cycle of enterprise collaboration including the pre-creation,