Unisanta Science and Technology, **2016, 16, December**
Published Online 2016 Vol.5 N°3 http://periodicos.unisanta.br/index.php/sat)

UNISANTA
Science and Technology
ISSN 2317-1316

Supply Chain Risk Management Framework for Virtual Enterprises: A Theoretical Approach

Maurício Fontoura Blos[1] and Sérgio Luiz Hoeflich[2]

[1] UNISANTA – Santa Cecília University
Department of Postgraduate studies – Master Program in Mechanical engineering -PPGEMec
Rua Oswaldo Cruz, 266 – Santos-SP, Brasil

[2] Polytechnic School of the University of São Paulo
Department of Electronics.
Av.Prof.Luciano Gualberto, n. 158 – São Paulo-SP - Brasil

Received November, 2015

Abstract: This paper considers risks of goods supplied in virtual enterprise (VE) and develops a supply chain risk management (SCRM) framework based on ISO/IEC27036 (information security for supplier relationship) and ISO28000 (specification for security management systems for the supply chain), aligned with ISO31000 (risk management and risk assessment techniques) and ANSИSA-95 (enterprise-control system integration). The developed framework is suitable for managing the risks of supplied goods for virtual enterprises (VEs); thus making the supply chain process more robust and resilient.

Keywords: Supply Chain Risk Management, Virtual Enterprise, Resilient.

Um Framework de Gerenciamento de Riscos da Cadeia de Suprimentos para Empresas Virtuais: Um Estudo Teórico

Resumo: Este artigo considera as mercadorias fornecidas em uma empresa virtual (EV) e desenvolve um framework de gerenciamento de riscos da cadeia de suprimento com base na ISO/IEC27036 (Segurança de Informação no relacionamento com Fornecedores) e na ISO28000 (Sistemas de Gestão de Segurança), alinhado com a ISO31000 (Gerenciamento de Riscos – Princípios e Diretrizes) e a ANSИSA-95 (Integração de Sistemas Empresarial de Controle). O desenvolvimento do Framework é adequado para o gerenciamento dos riscos das mercadorias fornecidas para uma EV e desta forma, fazendo que o processo da cadeia de suprimentos seja robusto e resiliente.

Palavras chave*:* gerenciamento de riscos, cadeia de suprimento, empresa Virtual, Resiliente.

1. Introduction

The virtual enterprise (VE) model has been identified as the best structure in the context of flexibility and ICTs usage (Blecker and Neuman, 2000; Choi et al., 2008; Pollalis and Dimitriou, 2008). More and more companies are geographically dispersed, and goods supplied are facing risk due to growing disruptive events (Sheffi, 2001; Revilla and Sáenz, 2013; Park et al., 2013). Under this circumstance, supply chain risk management (SCRM) has emerged (Chopra and Sodhi, 2004; Sodhi, et al., 2012; March and Shapira, 1987 ; Sitkin and Pablo, 1992; Zsidisin, 2003; Zsidisin et al., 1999). In dealing with the increasing problems for goods supply in the VE, a VE supply chain risk management framework is necessary.

The remaining sections of this paper are organized as follows: Section 2 gives the fundamental concepts. Section 3 discusses the proposed framework. Finally, section 4 presents the conclusions and future research.

2. Fundamental Concepts

In this section, a fundamental concepts related to risks in supply chains, VE, risk and security norms (ISO31000, ISO28000 and ISO27036) are discussed.

It supports supply chain and the ANSI / ISA-95 for developing an automated interface between enterprise and control systems.

2.1 Risks in Supply Chain

The classifications of risk in Supply Chains (SCs) have been clustered into different groups, but do not have a standardized framework (Chopra and Meindl, 2007; Jütner, 2005; Tang, 2006b). Among the risks types in the supply chains are disruptions resulted from natural disasters, supplier bankruptcy, labor disputes, war, terrorism attacks and socioeconomic political instability (Chopra and Meindl, 2007; Craighead et al., 2007; Hendricks and Singhal, 2005c; Kleindorfer and Saad, 2005). In our literature survey, we found that different sources for disruption risks are suggested by researchers, and many of them think that disruption risks generally have a low probability. Some papers refer to them as "catastrophic events" (Knemeyer, 2009).

They can seriously disrupt or delay material, information and cash flows; they can ruin sales, increase costs (or both) and the potential for a large loss. How a company overcomes such threats depends on the type of disruption and the organization's preparedness (e.g. supply chain continuity management or supply chain resilience management). Furthermore, companies need to assess their supply chain risk management to drive transparency throughout the supply chain. Based on the Figure 1, we purpose a supply chain risk framework and how it works.

2.2 The Virtual Enterprise (VE)

According to Cunha and Putnik (2006); Beckett (2008); Cao and Hoffman (2011); and Esposito and Evangelista (2014), VEs are alliances of interdependent businesses processes or companies where each participant contributes to its essential competence in areas such as: projects, manufacturing and distribution. In this context, the project, the development, the transportation, the manufacturing and the storage of goods are distributed geographically (Liang et al., 2008). These alliances are temporary, and they are formed to explore the rapid changes of the market (Cao and Hoffman, 2011; Esposito and Evangelista, 2014). The concept of VE was proposed by Nagel and Dove (1991) in a report on the "21st manufacturing enterprise strategy"; it initially used "Virtual Company" as the term for VE. Camarinha-Matos et al. (1998) defines VE as the alliances of companies that are based on "virtualization of resources". Applegate et al. (1999) define VE as the alliances of companies based on "virtualization of functions", and DeSanctis and Monge (1999) define VE as the alliances of companies based on "virtualization of forms". Figure 2 is an example of VE.

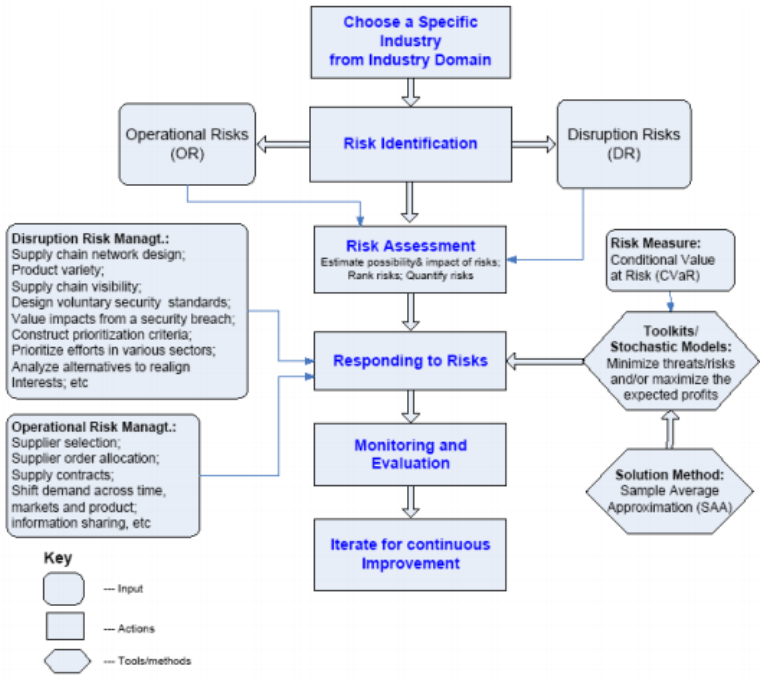

Figure 1. Example of Supply Chain Risk Management Framework (based on ISO31000).

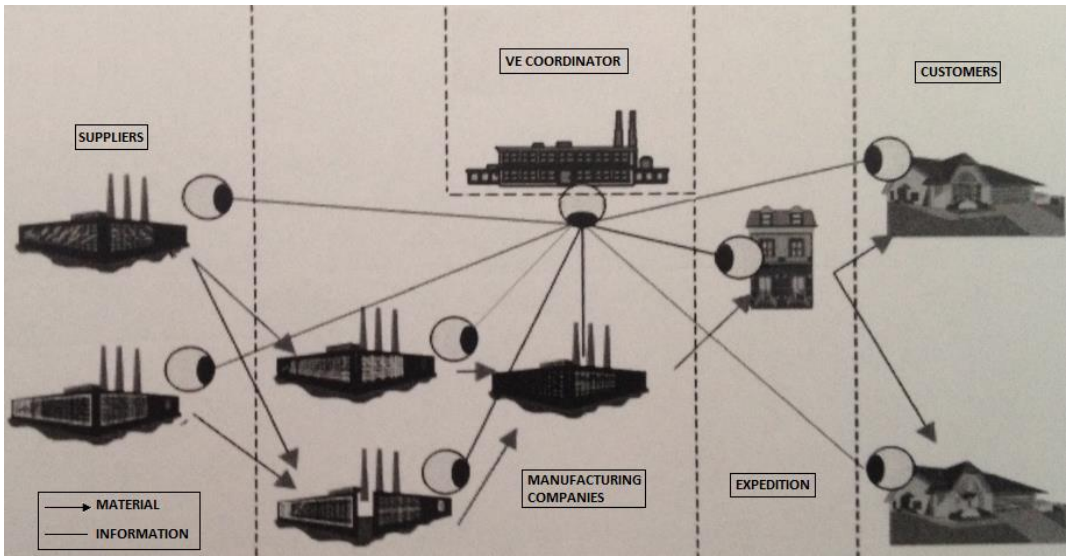

Figure 2. Example of Virtual Enterprise (VE).

In this example (Camarinha-Matos, L. M. and Afsarmanesh, H., 1999), we can see the material and information flow between partners (manufacturing company, suppliers, sales, clients, and the VE coordinator company).

2.3 The Risk Norm (ISO31000), the Security Supply Chain Norm (ISO28000), the Information Security for Supply Chain Norm (ISO27036) and the Enterprise-Control System Integration Norm (ANSI / ISA-95)

Since risks in supply chains result in the probability of financial losses and uncertainties (Leitch, M., 2010; Purdy, G., 2010), ISO 31000 can provide a foundation for supply chain managers to link SCRM and enterprise risk management (ERM) to secure an efficient supply chain management (SCM). ISO 31000 (ISO31000:2009) provides principles and generic guidelines on risk management; it is a universally recognized paradigm for practitioners and companies employing risk. ISO/IEC 27036 (ISO / IEC27036-1, 2, 3: 2013) allows one to enforce information security and reduce the possible fraud risks, information losses or disclosure that can disrupt the supply chains. In general, ISO 28000 and its actualizations (ISO / PAS 2008:2015, ISO28001:2007, ISO28002: 2007, ISO28003: 2007, ISO28004-1: 2007, ISO28004-2,3,4:2014) allow a supplier to ensure the necessary processes to mitigate risk and to promote resilience.

The ANSI*/*ISA-95 is the international standard from the international society of automation for developing an automated interface between enterprise and control systems. [47] proposed the addition of production control planning as part of the ANSI*/*ISA-95 in the VE. In our study, we propose the supply chain control planning as part of the ANSI*/*ISA-95 for the VE.

The importance of the risk norm (ISO31000), the supply chain security norm (ISO28000), the information security in supply chain norm (ISO/IEC 27036) and the norm of automated interface between enterprise and control systems (ANSI / ISA-95) are primordial to build the proposed framework (for managing supply chain risks of the owners and partners of the VE). Those norms are linked with the VE.

2.4 The Proposed Framework

The proposed framework is conceptualized in Figure 3 which depicts the owner and partners of VE. They share the same information from the ISO31000, ISO28000, ISO/IEC 27036 and the ANSI/ISA-95. Furthermore, all involved in the VE have the condition to manage supply chain risks for the goods supplied, following the premise that all manufacturers can be suppliers.

The proposed framework is divided into two layers; the first one is the VE-SCRM coordinator and the partners form the second layer. The owner is the dominating decision maker and the partners have to work according

to the owner's decision. In order to derive optimal decision, both owner and partners must follow the norms from Section 2.3.

Based on Figure 3, the first layer (owner) consists of information related to the purchase orders from all the suppliers. The second layer (several partners) consists of purchase orders to be supplied for each local planning service distributed in each local partner (supplier).

The first layer (owner) orchestrates each good supplied (in a cloud computing environment) and works closely with the second layer (several partners) the risks related to the supplied goods. Furthermore, this developed framework links Figures 1 and 2 to form the SCRM Framework for a VE (Figure 3). The developed framework is suitable for managing the risks of the goods supplied by/for virtual enterprise, making the supply chain processes more robust and resilient.

3. Conclusion

A framework of SCRM for a VE is developed to link SCRM with a VE. The framework shows the collaborative networks (CNs) of productive systems and supplier systems. The norm ANSI*/*ISA-95 is used by several companies to integrate systems (e.g. Enterprise Resource Planning). Furthermore, we proposed the supply chain control planning as part of the ANSI*/*ISA-95 in the context of VE.

The developed framework is also based on ISO/IEC27036 (information security for supplier relationship) and ISO28000 (specification for security management systems for the supply chain) that are aligned with ISO31000 (risk management and risk assessment techniques). They are suitable for managing the supply chain risks of the virtual enterprise, turning the supply chain processes more robust and resilient.

The first layer (owner) is composed of the information related to the purchase orders from all the suppliers. The second layer (several partners) is composed of the purchase orders to be supplied for each local planning service distributed in each local partner (supplier). The first layer (owner) orchestrates each good supplied and can manage together with the second layer (several partners) the risks related to the supplied goods. Furthermore, this developed framework makes a link of Figures 1 and 2 to form the SCRM Framework for VEs (Fig. 3). For future work, the study can be extended to the supply chain risk (SCR) mitigation for VEs in the context of the Industry 4.0.

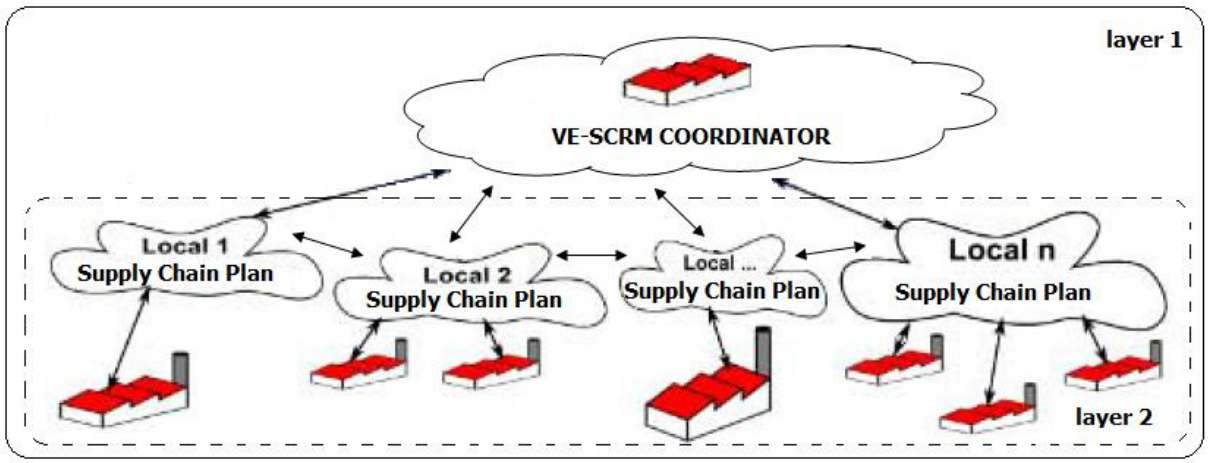

Figure 3. Supply Chain Risk Management Framework for Virtual Enterprises (adapted from Pessoa, 2015).

References

1. ANSI. ANSI / ISA-95.00.01-2010. Enterprise-Control System Integration. Part 1: Models and Terminology.
2. ANSI. ANSI / ISA-95.00.03-2005. Enterprise-Control System Integration. Part 3: Activity Models of Manufacturing Operations Management.
3. Applegate, L. M. ; McNekkey, J. L.; and McFarlan, F. W. (1999). Corporate Information System Management: Text and Cases. Irwin Professional Pub.
4. Beckett, R. C. (2008). Utilizing and Adaptation of the Absorptive Capacity Concept in a Virtual Enterprise Market Context. International Journal of Production Research. V.46 (5), pp.1243-1252.
5. Blecker, T.H. and Neuman, R. (2000). Interorganizational knowledge management - some perspectives for knowledge oriented strategic management in virtual organization. In: Malhotra, Y. (Ed.), Knowledge Management in Virtual Organization. Idea Group Publishing, Hershey London, pp. 63–83.
6. Calderon, P. (2014). 31 Success Secrets, 31 most asked questions on ISO31000 – What you need to know, Publisher: Emereo Publishing.
7. Camarinha-Matos, L. M. and Afsarmanesh, H. (1999). The Virtual Enterprise Concepts. Proceedings of the IFIP TC5 WG5.3 / PRODNET Working Conference on Infrastructures for Virtual Enterprises: Networking Industrial Enterprises. pp.3-14.
8. Camarinha-Matos, L. M.; Afsarmanesh, H.; Garita, C.; and Lima, C. (1998). Towards an Architecture for Virtual Enterprises. Journal of Intelligent Manufacturing. Springer Netherlands. V.9, pp.189-199.
9. Cao, Q. and Hoffman, J. J. (2011). Alignment of Virtual Enterprise, Information Technology, and Performance: An Empirical Study. International Journal of Production Research. V.49 (4), pp.1127-1149.
10. Choi, Y., Kang, D., Chae, H., and Kim, K. (2008). An enterprise architecture framework for collaboration of virtual enterprise chains. International Journal of Advanced Manufacturing Technology V. 35, pp.1065–1078
11. Chopra, S. and Meindl, P. (2007), Supply Chain Management - Strategy, Planning, and Operation, 3rd Ed. Prentice Hall, Upper Saddle River, NJ, USA.
12. Chopra, S. and Sodhi, M. (2004). Managing risk to avoid supply chain breakdown, MIT Sloan Management Review. V. 46 (1), pp. 53– 62.
13. Craighead, C. W., Blackhurst, J. Rungtusanathan, M. J. and Handfield, R. B. (2007). The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities. Decision Sciences, 38(1), pp. 131 -156.
14. Cunha, M. M. and Putnik, G. D. (2007). Identification of the Domain of Opportunities for a Market of Resources for Virtual Enterprise Integration. International Journal of Production Research. V.44 (12), pp.2277-2298.
15. DeSanctis, G. and Monge, P. (1999). Introduction to the Special Issue: Communication Processes for Virtual Organizations. Organization Science. Institute for Operations Research and the Management Sciences. V.10 (6), pp.693-703.
16. Esposito, E. and Evangelista, P. (2014). Investigating Virtual Enterprise Models: Literature Review and Empirical Findings. International Journal of Production Economics. V.148, pp.145-157.
17. Hendricks, K. & Singhal, V. R. (2005c). An empirical analysis of the effect of supply chain disruption on longrun stock price performance and equity risk of the firm. Production and Operations Management, 14(1), pp.35-52.
18. ISO/IEC27036-1:2013. Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts. ISO. Paperback – 2013.
19. ISO/IEC27036-2:2013. Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements. ISO. Paperback – 2013.
20. ISO/IEC27036-3:2013. Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security. ISO. Paperback - 2013.
21. ISO/PAS28000:2005. Specification for security management systems for the supply chain. ISO. Paperback – 2007
22. ISO28001:2007. Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance. ISO. Paperback – 2007.
23. ISO28002:2007. Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use. ISO. Paperback – 2007.
24. ISO28003:2007. Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems. ISO. Paperback - 2007.
25. ISO28004-1:2007. Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles. ISO. Paperback – 2007.

 Unisanta Science and Technology **(161-166) p.p. ISSN 2317-1316**

26. ISO28004-2:2014. Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations. ISO. Paperback – 2014.
27. ISO28004-3:2014. Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 3: Additional specific guidance for adopting ISO28000 for use by medium and small businesses (other than marine ports). ISO. Paperback – 2014.
28. ISO28004-4:2014. Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective. ISO. Paperback – 2014.
29. ISO31000:2009. Risk management — Principles and guidelines. ISO. Paperback – 2009.
30. Jütner, Uta. (2005), Supply Chain Risk Management – Understanding the Business Requirements from a Practitioner Perspective. International Journal of Logistics Management. 16(1), pp.120-141.
31. Kleindorfer, P. R. & Saad, G. H. (2005). Managing disruption risks in supply chain. Production and Operation Management. 14(1), pp.53-68.
32. Knemeyer, A., Zinn, w., & Eroglu, C., (2009). Proactive Planning for Catastrophic Events in Supply Chain. Journal of Operations Management. 27(2), pp.141 -153.
33. Leitch, M. ISO 31000:2009 - The New International Standard on Risk Management. Risk Analysis (2010); 30 (6), pp.887 - 92.
34. Liang, F.; Fung, R.Y.K.; Jiang, Z.; and Wong, T.N. (2008). A Hybrid Control Architecture and Coordination Mechanism in Virtual Manufacturing Enterprise. International Journal of Production Research, 46(13), pp.3641-3663.
35. March, J. and Shapira, Z. (1987). Managerial perspectives on risk and risk taking, Manag ement Science. V. 33 (11), pp. 1404– 1418.
36. Nagel, R. and Dove, R. (1991). 21st Century Manufacturing Enterprise Strategy: An Industry Led View.
37. Park, Young Won; Hong, Paul and Roh, James Jungbal. (2013). Supply Chain lessons from the Catastrophic Natural Disaster in Japan. Business Horizons. V. 56, pp.75-85.
38. Pessoa, M. A. O. (2015). PhD Thesis: Architecture of Planning and Controlling System of Production in the context of Virtual Enterprise (in Portuguese). Polytechnic School of the University of São Paulo.
39. Pollalis, Y.A. and Dimitriou, N.K. (2008). Knowledge Management in virtual enterprises: a systemic multi-methodology towards the strategic use of information. International Journal of Information Management. V. 28 (4), pp.305–321.
40. Purdy, G. ISO 31000:2009 - Setting a New Standard for Risk Management. Risk Analysis (2010); 30:881 - 6.
41. Revilla, Elena and Sáenz, María Jesús (2013). Supply chain disruption management: Global convergence vs national specifi city. Journal of Business Research. xxx, xxx-xxx.
42. Sheffi, Yossi (2001). Supply Chain Management under the threat of International Terrorism. The International Journal of Logistics Management. V. 12 (2), 1-11.
43. Sitkin, S.B. and Pablo, A.L. (1992). Reconceptualizing the determinants of risk behavior, Aca demy of Management Review. V. 17 (1), pp. 9– 38.
44. Sodhi, M.S., Son, B.-G. and Tang, C.S. (2012), "Researchers' perspectives on supply chain risk management", Production and Operations Management, V. 21 (1), pp. 1-13.
45. Tang, C. S. (2006b). Perspectives in Supply Chain Risk Management. International Journal of Production Economics. 103(2), pp. 451-488.
46. Zsidisin, G.A. (2003). A grounded definition of supply risk, Journal of Purchasing and Supply Management 9 (5/6), pp. 217–224.
47. Zsidisin, G.A.; Panelli, A. and Upton, R. (1999). Purchasing organization involvement in risk assessments, contingency plans and risk management: an exploratory study, Supply Chain Management; An International Journal. V. 5 (4), pp.187–197.

