# CONSIDERATIONS ON RISK IN SUPPLY CHAIN MANAGEMENT INFORMATION SYSTEMS IMPLEMENTATION

**Valentin-Petru Măzăreanu***
*Alexandru Ioan Cuza University from Iaşi, Romania*

**Abstract**
Innovation in information and communication technologies resulted in the digital revolution. This kind of revolution is changing the way people work, learn, communicate and manage their businesses. Due to the need to achieve the competitive advantage and to meet the business requirements, we are witnessing an increasing shift from business to e-business and mobile business. In this kind of world solutions like Supply Chain Management (SCM) are increasingly appearing.
The business success depends on how effective the information system works. Any interruption of the information system will inevitably lead to business loss. To ensure the successful implementation of a SCM project it is necessary to study even from the early stages which are the possible actions / risks / obstacles which might damage in one way or another the execution of the project.
The role of the literature and case studies review in the field of interest is undeniable because it provides us with access to the so-called *lessons-learned*. By using this approach, in this paper, we present the most common risks and risk sources encountered in the implementation projects of SCM type information systems. We also propose a risk identification framework that can be used in the early stages of the implementation project of a Supply Chain Management information system.

**Keywords:** Supply Chain Management, risk, risk management, integrated information system

**JEL Classification:** D81, G32

## Introduction

We cannot ignore any longer the fact that the way in which businesses are managed is changing. The literature mentions about these changes using superlatives as technological change, revolutionary change, a new paradigm, a tsunami of changes and so forth. Obviously, these changes are manifested at the level of organization as well. Tapscott (1996) initiated a study in order to review all the expressions used in the literature to describe this new organization. He identified the following concepts: networked

* Author's contact: e-mail: vali.mazareanu@feaa.uaic.ro

organization (mentioned by Peter Druker), learning organization (Peter Senge), virtual corporation (Davidow and Malone), relational organization (Peter Keene), crazy organization (Tom Peters), cluster organization (Quinn Mills), interactions and human networking (Charles Savage), democratic corporation (Russell Ackoff), intelligent enterprise (James Brian Quinn) and reengineered corporation (Michael Hammer and James Champy).

The fundamental changes are essential. The digital economy has created new business models such as e-business, e-banking, e-government etc. Obviously, the list is not closed. In fact, this world of "e-" is practically endless and almost any human activity can be "translated" into electronic format. We can rightly say that we live in times when we are involved in e-Business, we buy from e-Mall, we pay our taxes using e-Tax systems, we "live" in an e-Democracy and our government is e-governing us. We implement solutions such as business intelligence (BI), geographic information systems (GIS), enterprise resource planning systems (ERP), customer relationship management (CRM) and so forth. We live in a society where the presence of the computer cannot be ignored any longer. It is a component that gains an increasingly greater role in the human activity, making our work more efficient and (maybe) more enjoyable.

It is evident, therefore, that the business world is dominated by the "*e* Revolution". Furthermore, a new concept emerged in this field: e-business is business (Deise, et al., 2000). And businesses are just at the beginning, if we are to take into account the emergence of wireless technologies and mobile business.

However, new solutions bring new forms of risks! The computer viruses have become increasingly proficient, being now able to expand on the mobile operating systems or on vehicle on board computers. Email spam or web spam (Prieto, et al, 2012) attacks have multiplied and become increasingly sophisticated. Banking and financial institutions fall victims of phishing scams and so the user of the internet banking system is affected. Security systems start using smart cards, biometric or behaviometric systems (based on user behavior analysis).

The conclusion follows easily: the adoption of information systems increases the number of vulnerabilities (Jüttner, 2005), the risks faced by an organization have diversified tremendously and continue to diversify as the time goes on, so the measures to combat these risks must be appropriate.

This study aims to identify and centralize the most common risks and risk sources encountered in the implementation projects of SCM information systems. Based on these, we propose a risks identification framework that can be used in the early stages of the implementation project of the Supply Chain Management information system. The research methodology used to achieve the objectives was based on literature and case studies review.

## 1. About the risks in SCM implementation projects

Innovation in information and communication technologies resulted in the digital revolution. This kind of revolution is changing the way people work, learn, communicate and manage their businesses. The essential elements of the digital revolution are digitization, intensive use of information and communication technologies, codification of knowledge, transformation of the information in products, the advent of new ways of

organizing work and production (Sharma, 2005). This implies that most of the information and services are available online (hence the risks). Wide access to computer networks, intranets and the Internet and new skills to work and live in the information society represents the basis of the digital economy.

The developments occurred in the area of information and communication technologies have allowed many organizations to implement information systems that connect their own system to that of the clients or suppliers. According to a study (Maguire, 2002), in many situations this connection has allowed obtaining a competitive advantage in relation to the other participants on the market. In other cases, the competitive advantage was obtained as result of business intelligence systems implementation that offers the image of the business tendency based on the analysed information or as the result of the interpretation of the results obtained following the information geo-referencing with the help of geographic information systems.

Due to the need to achieve the competitive advantage and to meet the business requirements, we are increasingly witnessing a shift from business to e-business and mobile business. In this kind of world solutions like (Social) Customer Relationship Management, Enterprise Resource Planning or Supply Chain Management (SCM) are appearing increasingly. Most of the SCM implementation projects (applies to all information systems) follow a well-structured plan, a methodology (e.g. ASAP, The Total Solution, The Fast Track Work plan) that tries to take into account as much risk as it can.

In any each of the mentioned cases, the success depends on the efficiency of the information system. Using modern information systems (e.g. decision support systems, systems analysis) has become indispensable for designing and managing complex SCM solutions. Any interruption of the information system will inevitably lead to business losses. In order to avoid this situation, risk solutions are designed and implemented; risk solutions such as decision support systems specialized in SCM (Giannakis and Louis, 2011), analytical hierarchic process (Schoenherr, Tummala and Harrison, 2008; Gaudenzi and Borghesi, 2006), HOR methodologies (Pujawan and Geraldin, 2009), solutions that are based on Petri nets models (Tuncel and Alpan, 2010) or dedicated risk management approach called SCRM - supply chain risk management (Colicchia and Strozzi, 2012; Lavastre, Gunasekaran and Spalanzani, 2012; Tumala and Schoenherr, 2011; Neiger, Rotaru and Churilov, 2009).

To ensure the successful implementation of a SCM project, it is necessary, even from the early stages, to study which are the possible advantages/disadvantages (Surcel and Bologa, 2008), recommended actions/strategies/principles (Knolmayer, Mertens and Zeier, 2000; Fotache and Hurbean, 2006), risks/obstacles (Kalakota and Robinson, 2001; Fawcett, Magnan and McCarter, 2008) that might damage in one way or another the execution of the project. The importance of risk management is outlined.

The role of literature and case studies review in the field of interest is undeniable because it provides us with the access to the so-called *lessons-learned*. We synthesize the research findings in the table below (table no. 1). Nnote that we only have selected for presentation the top 4-5 risks for each analysed study.

**Table no. 1: A synthesis of the risks occurred in information systems implementation projects**

| No. | Author of the study | Risk Category | Risk Management Plan |
|---|---|---|---|
| 1. | **Infosys** (Jalote, 2002) | Lack of specialized personnel in the technical field | Make estimates taking into account the initial learning period;<br>The existence of extra resources;<br>Conduct training programs. |
| | | Too many changes of the requirements | Obtaining a final decision on the initial requirements;<br>Making the client understand that change will affect planed requirements;<br>Define a requirements change management procedure;<br>Negotiate the payment in accordance with the current effort. |
| | | Unclear requirements | Use experience and logic to make assumptions, but inform the client;<br>Obtain a final decision;<br>Develop a prototype and let the client review requirements. |
| | | Routine of the specialized personnel | Provide more resources in the key points of the project;<br>Organize team-building sessions;<br>Rotation in job attributions;<br>Keep extra resources;<br>Documentation for each job;<br>Follow strict guidelines and configuration of management process. |
| | | Constraints from outside | Drafting of disadvantages and negotiation with the personnel in order to force a decision;<br>Risk identification;<br>Tracking specific response plans. |
| 2. | **Standish Group** (Opran, Paraipan and Stan, 2004) | Incomplete requirements of the project | - not stated |
| | | Insufficient involvement of the project partners | |
| | | Insufficient resources | |
| | | Unrealistic estimates of project results | |
| | | Insufficient executive support | |
| 3. | **Barry Boehm** (Kwak and Stoddard, 2008) | Incompetence of staff | - not stated |
| | | Unrealistic budget and schedule | |
| | | Developing the wrong functions and properties | |
| | | Developing the wrong user interface | |
| | | Adding more functionality than needed | |
| 4. | **Futrell, Robert, T.** (Futrell, Shafer and Shafer, 2002) | Few expert engineers | Contract other experts. |
| | | Tight design deadline | Delphi estimates. |
| | | Poor organization of the reporting function | Customer review. |
| | | Different interfaces | Customer review. |
| | | New requirements | Budget review. |

| No. | Author of the study | Risk Category | Risk Management Plan |
|---|---|---|---|
| **5.** | **The ITA Board** (Missouri State Government, 2007) | Personnel availability | Ensuring that the specifications contain sufficient information to allow new staff to understand the system. |
| | | Personnel abilities and competencies | Anticipating the required level of skill. |
| | | Schedule risk | Breaking the project into smaller segments to ensure the preservation of the schedule. |
| | | Costs (budget) | Cost review to ensure that all activities are reflected. |
| | | Change management and control | Ensuring that the change control process is implemented to limit core business changes. |
| **6.** | **Mursu, A., Lyytinen, K., Soriyan, HA., Korpela, M.** (Mursu, et al., 2003) | Misunderstanding of the requirements by the team members / organization | - not stated |
| | | Lack of process / methodology developed effectively | |
| | | Lack of knowledge of the personnel | |
| | | Lack of abilities of the personnel | |
| | | No funding | |
| **7.** | **Barki, H., Rivard, S., Talbot, J.** (Brett, 2007) | Technical innovations that require experience in technology | - not stated |
| | | Diversity in the team | |
| | | Team experience | |
| | | Leader experience | |
| | | Interpersonal and preference conflicts | |
| **9.** | **Borghesi, A.** (Borghesi, 2003) | International legislation | - not stated |
| | | Continuous development in technology | |
| | | Security of transactions | |
| | | Infrastructure | |
| | | The nature of the product | |
| **10.** | **DeMarco, T.** (Futrell, Shafer and Shafer, 2002) | Requirements misunderstanding | - not stated |
| | | Lack of historical data (used in estimates) | |
| | | Lack of an evaluation standard | |
| | | Misunderstandings between project stakeholders and customers | |
| | | Failure to report mistakes | |
| | | Organization management | |
| | | Clients risk | |
| | | Budget risk | |
| | | Schedule risk | |
| **11.** | **Net Com** (Krantz, 2006) | Failure to understand the project | - not stated |
| | | Failure in the appointment of a project sponsor | |
| | | Failure in the appointment of a project manager | |
| | | Failure to define project objectives | |

| No. | Author of the study | Risk Category | Risk Management Plan |
|---|---|---|---|
| | | Failure in obtaining a consent for the project from the key people | |
| 12 | **Tummala R. and Schoenherr T.** (Tummala and Schoenherr, 2011) | Demand risks | - not stated<br>- a Supply Chain Risk Management Process (SCRMP) is proposed |
| | | Delay risks | |
| | | Disruption risks | |
| | | Inventory risks | |
| | | Manufacturing (process) breakdown risks | |
| | | Physical plant (capacity) risks | |
| | | Supply (procurement) risks | |
| | | System risks | |
| | | Sovereign risks | |
| | | Transportation risks | |

We see a pattern, which is that the human actions are in the first positions of the charts with the risks occurring in the information systems implementation projects. The human component must be taken into account at least from two points of view: human, as a source of attack to the information system (e.g. outside attacks, inside attacks – ill intended persons, unprepared persons etc.) and the risk generated by the status of key position of a human resource within the system (e.g. the effects caused by disease, death, leaving the team etc.). For a deeper analysis of human factor risks see Măzăreanu (2012).

It is certain that in (information) risk management (for the matter, the entire field of information technology follows the same pattern) knowledge and practice advance quickly (Janczewski, 2000). Under these conditions, there is always a demand for updated materials.

## 2. A risk identification framework for SCM projects

Risks arise in all socio-economic activities but in different forms depending on the type, mode of expression and size. After analyzing the case studies (real implementations, best practices, lesson learned) and reviewing the literature in the field, we present in table no. 2 a risk classification model that takes into account the risk source.

**Table no. 2: Overview of sources of risk and risk classification**

| Risk Source | Classification | Examples from SCM implementation projects |
|---|---|---|
| **Human factor** | - human behavior risks (Narasimhan and Talluri, 2009);<br>- human psychological factors risks;<br>- risks from individual activities;<br>- risks from user involvement and training (Huang, et al., 2004). | - inability to complete a task on time, poor quality of staff;<br>- unrealistic expectations, focus on details and losing sight of the objectives;<br>- inefficient communication with the user, insufficient training of the end-user. |
| **Organization** | - strategic: risks related to the organization's strategy (Harland, et al., 2007; Yaibuathet, Enkawa and Suzuki, 2008);<br>- operational: risks affecting the | - risks related to the intellectual capital of the company, changes taking place at the macroeconomic level;<br>- fraud, insufficient resources, business process reengineering failures; |

| Risk Source | Classification | Examples from SCM implementation projects |
|---|---|---|
| | current activities of the company (Dima, 2009);<br>- financial: risks related to the financial aspects of the company (Blos, et al., 2009);<br>- hazard: unpredictable events (usually caused by nature). | - lack of liquidity, failure in paying the contractual obligations by the business partners;<br>- foreign exchange risk (Liu and Nagurney, 2011);<br>- natural disasters, fires (Speier, et al., 2011). |
| **Leadership style** | - risks arising from the differences in management policies;<br>- risks arising from the management activities and controls;<br>- risk arising from organization management skills, poor management (Onofrei and Lupu, 2012). | - lack of executive support;<br>- changes in requirements, poor leadership;<br>- failure to attract qualified staff, insufficient knowledge. |
| **External Environment** | - risks arising from economic, social, political and environmental circumstances (Olson and Wu, 2010; Ritchie and Brindley, 2007). | - changing market conditions, harmful competition actions, outdated software;<br>- terrorism, state of war (Olson and Wu, 2010). |
| **IT&C Resources of the Organization** | - risks arising from technical and technological problems;<br>- risks arising from the software design and implementation;<br>- risks arising from the administration of information (Pereira, 2009). | - inadequate documentation, applications are implemented without meeting the initial requirements, inadequate know how (Oprea, 2001);<br>- instability of the current technology, inability to connect to the legacy systems;<br>- misunderstanding the change requirements, systems are not integrated. |
| **Relationship with third parties** | - risks arising from legal (Shaohan, Minjoon and Zhilin, 2010, Child, Chung and Davis, 2003) and contractual (Baccarin, Salm and Love, 2004) relations;<br>- partnerships with SMEs (Pujawan and Geraldin, 2009; Finch, 2004)<br>- risks arising from reputation damage. | - inadequate performance of third parties, inadequate protection of intellectual property tensions between clients and contractors;<br>- increased confidence in providers (Narasimhan and Talluri, 2009; Wagna and Bode, 2006);<br>- breaches or non-compliance with the law. |

The model and the synthesis presented in the table 1 may help us in shaping the sources of risk and hence a risk identification framework that can be used in SCM implementation projects.

Under these conditions, in the Figure no. 1 we illustrated a risk identification framework. This framework takes into account the classification of risk based on the factor that contributes to its appearance and its source, either internal or external to the organization. The predictable or unpredictable nature of the dangerous event is also taken into account.

This representation is just an incipient framework because, in our opinion, there cannot be a complete model that can reveal all sources and types of risks. Even so, such items and groups of interest can be easily extracted from the organization's previous information systems implementation projects (lessons learned) or from different "top 10 risks" of various institutions, organizations, security centers, and so forth. (Brandon, 2005; Futrell, Shafer and Shafer, 2002; Tchankova, 2002).

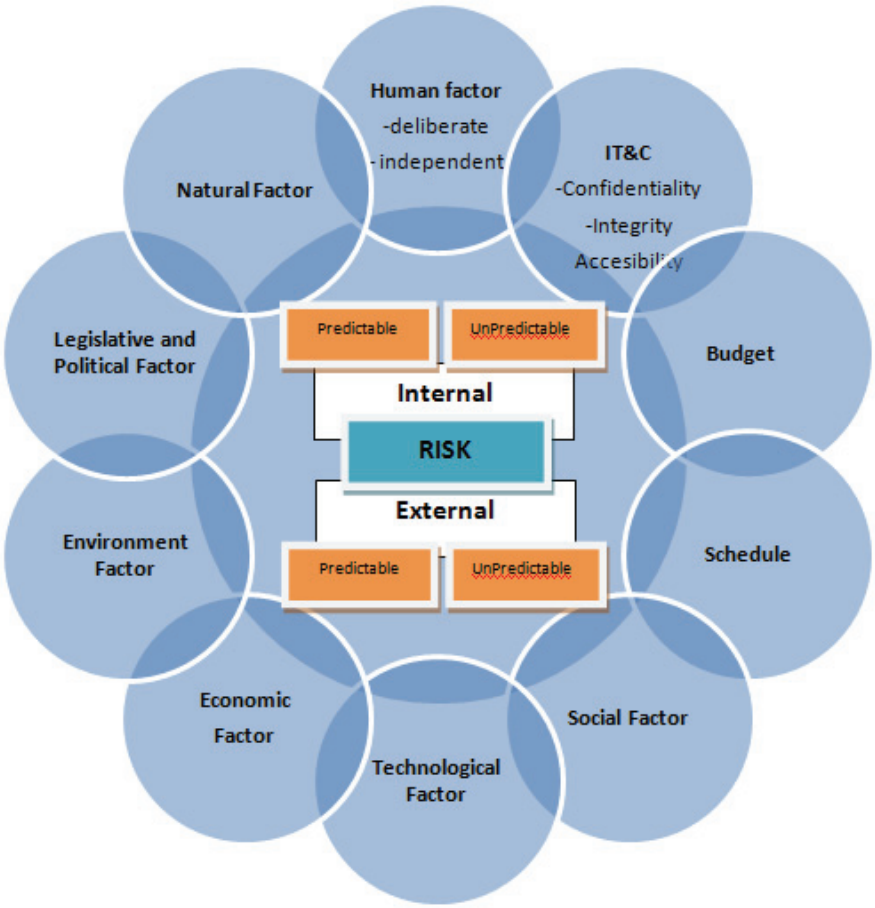


**Figure no. 1: A risk identification framework for SCM implementation projects**

Source: Măzăreanu, 2010, p.73

**Conclusions**

By realizing a literature and case studies review, this study has identified and centralized the most common risks and risk sources encountered in the implementation projects of SCM information systems. Based on these, we have proposed a risks identification framework that can be used in the early stages of the implementation project of the Supply Chain Management information system.

The personal computer is present in almost all areas of activity, assisting and facilitating the work. On every passing day, the user collects data, processes it, filters it and stores it in different environments. Data are analyzed for gathering information useful in carrying out the work. The amount of information increases and almost imperceptibly a change appears

in the above paradigm: the user becomes dependent on the information. Placed in the competitive environment (and this is not necessarily about business, but also applies to research, science or education) the dependence on information becomes chronic. With the aggravation of the symptoms mentioned above and benefiting from the digitization of documents and the effects of Moore's law, increasingly more information is processed, stored and transmitted electronically, causing the changes in how the scientific research is conducted, in how the students work in laboratory and especially in the way companies approach their business. We are thus witnessing an electronic revolution, with all its benefits, but also with the dangers it entails.

The new information and communication technologies have forced a shift in the way businesses are managed towards electronic and mobile commerce/business solutions, to complex business process management or procurement and e-auctions solutions. The IT&C led to the rethinking of the government policies, causing specific electronic governance and democracy practices. In this way, the efficiency with which employees communicate, businesses operate, the government rules and citizens of countries are involved in managing the political process increased.

At the same time, the risk to the security of information and information systems increased. Compared with the printed documents, the information stored on electronic media can be easily accessed, altered or stolen. Attention now falls on confidentiality, integrity, availability and authenticity of information. If the storage is stolen, its owner would know immediately that they are at risk (e.g. advertising a trade secret or exposing the confidential data of a person holding a particular bank account) and should be able to estimate relatively quickly the loss and to suggest a recovery plan. More sensitive are those aspects related to imperceptible vulnerabilities that may expose information to the undetected attacker, unfair competitive intelligence, negligent loss of information and so forth. All these have far exceeded the boundaries of fiction and became real facts. Thus managers should be aware of these risks and the importance of implementing risk management plans. They should be especially aware that with the development of information and communication technologies the types of attacks will also evolve and the control measures that were implemented *yesterday* are now obsolete.

**Acknowledgements**

The results presents in this paper were obtained in the framework of the postdoctoral school programme financed by the *"Developing the Innovation Capacity and Improving the Impact of Research through Post-doctoral Programs - POSDRU/89/1.5/S/49944"* project.

**References**

Baccarini, D., Salm, G. and Love, P.E.D., 2004. Management of risks in information technology projects. *Journal of Industrial Management & Data Systems*, 104(4), p.287

Blos, M.,F., Quaddus, M., Wee, H.,M. and Watanabe, K., 2009. Supply chain risk management (SCRM): a case study on the automotive and electronic industries in Brazil. *Supply Chain Management: An International Journal*, 14(4), pp. 247 – 252

Borghesi, A., 2001. *Credit risk and the new economy*, [online] Available at: <http://www.arimas.it/papers.htm> [Accesed 25 July 2003]

Brandon, D., 2005. *Project management for modern information systems*. Hershey: IRM Press

Brett, T., 2007. *Managing risk with metrics - a term paper for the MJY team software risk management*, [online] Available at: < www.baz.com/kjordan/swse625> [Accessed 23 September 2007].

Child, J., Chung, L. and Davis, H., 2003. The performance of cross-border units in China: a test of natural selection, strategic choice and contingency theories. *Journal of International Business Studies,* 34 (3), pp. 242–254

Colicchia, C. and Strozzi, F., 2012. Supply chain risk management: a new methodology for a systematic literature review. *Supply Chain Management: An International Journal*, 17(4), pp. 403 - 418

Deise, M., V., Nowikow, C., King, P. and Wright, A., 2000. *Executive's Guide to E-Business – from tactics to strategy*, New York: John Wiley & Sons, INC

Dima, A., M., 2009. Operational risk assessment tools for quality management in banking services. *Amfiteatru Economic*, XI (26), pp. 364-372

Fawcett, S., E., Magnan, G.,M. and McCarter, M., W., 2008. Benefits, barriers, and bridges to effective supply chain management. *Supply Chain Management: An International Journal*, 13(1), pp. 35 - 48

Fotache, D. and Hurbean, L., 2006. Supply Chain Management: from linear interactions to networked processes. Informatica Economica, 4(40), pp. 73-77

Finch, P., 2004. Supply chain risk management. *Supply Chain Management: An International Journal*, 9(2), pp. 183 - 196

Futrell, R.T., Shafer, D.F. and Shafer, L.I., 2002. *Quality Software Project Management*. Software Quality Institute Series, Upper Saddle River: Prentice Hall PTR

Gaudenzi, B. and Borghesi, A., 2006. Managing risk in the supply chain using the AHP method. *The International Journal of Logistics Management*, 17(1), pp. 114-36.

Giannakis, M. and Louis, M., 2011. A multi agent based framework for supply chain risk management. *Journal of Purchasing & Supply Management*, 17, pp. 23–31

Harland, C.M., Caldwell, N.D., Powell, P. and Zheng, J., 2007. Barriers to supply chain information integration: SMEs adrift of eLands. *Journal of Operations Management*, 25, pp. 1234–1254

Huang, S.M., Chang, I.C., Li, S.H. and Lin, M.T., 2004. Assessing risk in ERP projects: identify and prioritize the factors. *Journal of Industrial Management & data Systems*, 104(8), p.685

Jalote, P., 2002. *Software Project Management in Practice*. Boston: Addison-Wesley

Janczewski, L., 2000. *Internet and Intranet Security Management: Risks and Solutions.* Hershey: Idea Group

Jüttner, U., 2005. Supply chain risk management: Understanding the business requirements from a practitioner perspective. *The International Journal of Logistics Management*, 16(1), pp. 120 - 141

Kalakota, R. and Robinson, M., 2001. *E-Business 2.0. Roadmap for Succes.* Boston: Addison-Wesley

Knolmayer, G., Mertens, P. and Zeier, A., 2000. Supply Chain Management auf der basis von SAP-System, Springer-Verlag, Berlin

Krantz , L., 2006. *An overview over project risk management*, [online] Available at: http://www.netcomuk.co.uk/~rtusler/project/riskprin.html [Accessed 21 August 2006]

Kwak, Y. and H., Stoddard, J., 2008. *Project risk management: lessons learned from software development environment*, [online] Available at: <http://www.software-engineer.org> [Accessed 12 April 2008]

Lavastre, O., Gunasekaran, A. and Spalanzani, A., 2012. Supply chain risk management in French companies. *Decision Support Systems*, 52, pp. 828–838

Liu, Z. and Nagurney, A., 2011. Supply chain outsourcing under exchange rate risk and competition. *Omega*, 39, pp. 539–549

Maguire, S., 2002. Identifying risks during information systems development: managing the process. *Journal of Information Management & Computer Security*, 10(3), p. 126

Măzăreanu, P.V., 2010. *Economia Digitală şi Managementul Riscurilor* Iasi:Tehnopress

Măzăreanu, P.V., 2012. About the human factor in risk management – primary source of uncertainty. *Journal of Information Systems & Operations Management*, 6(1), p.41

Missouri State Government, 2007. *Missouri IT Risk Management Manual*, [online] Available at:<http://oit.mo.gov/> [Accessed 13 April 2007]

Mursu, A., Lyytinen, K., Soriyan, HA and Korpela, M., 2003. Identifying software project risks in Nigeria: an International Comparative Study. *EJIS – European Journal of Information Systems*, 12( 3), pp. 182-188

Narasimhan, R. and Talluri, S., 2009. Perspectives on risk management in supply chains. *Journal of Operations Management*, 27, pp. 114–118

Neiger, D., Rotaru, K. and Churilov, L., 2009. Supply chain risk identification with value-focused process engineering. *Journal of Operations Management,* 27, pp.154–168

Olson, D., L. and Wu, D.,D., 2010. A review of enterprise risk management in supply chain. *Kybernetes*, 39(5), pp. 694 - 706

Onofrei, M. and Lupu, D., 2012. The management of economic decline and the dimension of organizational change. *Amfiteatru Economic*, XIV (32), pp. 470-484.

Opran, C., Paraipan, L. and Stan, S., 2004. *Managementul Riscului*, Bucure□ti: SNSPA

Oprea, D., 2001. *Managementul Proiectelor-teorie şi cazuri practice*. Iasi: Sedcom Libris

Pujawan, I.,N. and Geraldin, L., H., 2009. House of risk: a model for proactive supply chain risk management. *Business Process Management Journal*, 15(6), pp. 953 - 967

Pereira, J.V., 2009. The new supply chain's frontier: Information management. *International Journal of Information Management*, 29(5), pp. 372–379

Prieto, V.M, Alvarez, M., Lopez-Garcia, R. and Cacheda, F., 2012. Analysis and Detection of Web Spam by Means of Web Content. In: M.Salampasis, B. Larsen, ed. 2012. *IRFC 2012, LNSC* 7356. Berlin: Springer-Verlag, pp.43-57

Ritchie, B. and Brindley, C., 2007. An emergent framework for supply chain risk management and performance measurement. *Journal of the Operational Research Society*, 58, pp. 1398-411

Schoenherra, T., Tummalaa V.M.R. and Harrison, T.P., 2009. Assessing supply chain risks with the analytic hierarchy process: Providing decision support for the offshoring decision by a US manufacturing company. *Journal of Purchasing & Supply Management*, 14, pp. 100–111

Shaohan, C., Minjoon, J. and Zhilin, Y., 2010. Implementing supply chain information integration in China: The role of institutional forces and trust. *Journal of Operations Management*, 28, pp. 257–268

Sharma, S.K., 2005. Socio-economic impacts and influences of e-commerce in a digital economy. In: H.S., Kehal, V.P., Singh, ed. 2005. *Digital Economy: Impacts, influences and challenges*. Hershey: Idea group, p.4

Speiera, C., Whippleb, J.M., Clossc, D.J. and Vossd, M.D., 2011. Global supply chain design considerations: Mitigating product safety and security risks. Journal of Operations Management, 29, pp. 721–736

Surcel, T. and Bologa, R., 2008. The ERP capabilities for enhancing the logistic system integration. *Amfiteatru Economic*, X(24), pp. 84-93

Tapscott, D., 1996. *The Digital Economy – Promise and Peril in the Age of Networked Intelligence*. New York: McGraw-Hill

Tchankova, L., 2002. Risk Identification – Basic Stage in Risk Management. *Journal of Environmental, Management and Health*, 13(3), pp.290-297

Tummala, R. and Schoenherr, T., 2011. Assessing and managing risks using the Supply Chain Risk Management Process (SCRMP). *Supply Chain Management: An International Journal*, 16(6), pp. 474 - 483

Tuncel, G. and Alpan, G., 2010. Risk assessment and management for supply chain networks: A case study. *Computers in Industry*, 61, pp. 250–259

Wagne, S.M. and Bode, C., 2006. An empirical investigation into supply chain vulnerability. *Journal of Purchasing & Supply Management*, 12, pp.301–312

Yaibuathet, K., Enkawa, T. and Suzuki, S., 2008. Influences of institutional environment toward the development of supply chain management. *International Journal of Production Economics*, 115 (2), pp.262–271