Journal of Information Assurance and Security 2 (2007) 288-296

Security And Risk Management in Supply Chains

Youakim Badr[1] and Jean Stephan[2]

[1]National Institute of Applied Sciences – Lyon
INSA-Lyon, F-69621, France
youakim.badr@insa-lyon.fr

[2]Université Saint-Esprit - Kaslik
BP 446 Jounieh, Lebanon
jeanstephan@usek.edu.lb

Abstract: The reduction of risk constitutes a pillar of success in business. A crucial concern in any business activity includes the variable of risk due to security threats in information systems. Risks increase as the business increases in success and profit. Risk Management becomes a crucial part of every successful business model to deal with uncertain and risky socio-economic changes. Security concerns are a major player in minimizing risk in businesses by protecting its intangible resources and knowledge. The emergence of supply chains which coordinate organizations, people, activities, information and resources, dramatically increases risk crises. Efforts have resulted in process reference models, such as the Supply Chain Operations Reference (SCOR) which measures total supply chain performance. Although the SCOR model is designed to support supply chains of various complexities across multiple industries, it does not provide a basis for Risk Management in terms of the security of exchanged information and access control. Quantifying security risks in supply chains becomes a central challenge to be considered in risk management. This paper attempts to propose a framework to bridge the gap between security concerns and risk management in a supply chain, typically, the SCOR model. The framework extends risk management with security awareness by proposing roles for each process in SCOR. Its underlying approach focuses on the types of threats in SCOR implementation projects and applies empirical benchmarks to measure risks in processes with respect to the security-oriented framework.

Keywords: Supply Chain, SCOR, Security, Risk Management …

1. Introduction

Because of the complex interrelations of social, economic and manufacturing issues, risks occur at various levels of business, it might stem from numerous types of threats caused by the markets, technology, social networks, organizations and politics. On the other hand it involves all means available for humans (i.e. people, personnel and organizations). Strategies to recognize risk include transferring the risk to another party, avoiding the risk, reducing the negative effects, and accepting some or all of the consequences of a particular risk. Risk Management [1] aims to reduce crisis impact related to a particular domain.

The emergence of information and communication technologies allows disparate firms to not only exchange information but also manage the supply chain of suppliers and customers. Due to supply chains, firms can collaborate and coordinate their processes. Existing supply chain management models are enhanced by the means of a greater focus on processes and key indicators without taking into account Risk Management. Since the SCOR model [2] is considered a de facto standard for supply chains, its potential importance resides in the integration of concepts of business process reengineering and process measurement into a cross-functional framework.

Unfortunately, the SCOR model does not provide Risk Management support or best practices to analyze risks or a security framework to support risk management by taking into account the risk in exchanged data with partners or inside the firm's processes..

The SCOR model only focuses on enhancing productivity, eliminating waste, removing supply chain duplication and driving for cost improvement. All of these are crucial aspects of SCOR supply chain management. The mismanagement of the input and output of processes in the SCOR model leads to negative impacts on the flow of information and directly affect the outcome of these processes, which in turn decrease the overall performance.

This paper proposes a generic framework to extend the SCOR model in order to deal with risk management focusing on security of information.

The framework takes into consideration all levels of SCOR processes and in particular their input, output and best practices and reduces the gap between the SCOR model and Risk Management as follows:

- Risk identification: the framework attempts to identify potential categories of risks and their impacts on managing supply chain processes. It consequently deals with different security issues and their strategic and operational impacts on the decision making process.
- Risk due to Access Control: risk might emerge from inputs or outputs that link SCOR processes: some inputs might be linked to external and/or internal process outputs. Inputs and outputs should be controlled using different access control methods. Thus, the vertical flow of information between SCOR process levels mainly concerns the security policies inside the firm's organization whereas the horizontal flow of information also requires trust relationships and secure exchange with customers, suppliers and stakeholders.
- Time and spatial based risks: the organization of supply chains is dynamic and evolves over time and geographical locations. Risks can propagate through the supply chain with time and affect chronologically all resources and partners of the chain. The risk management of supply chains should take into account the forecasting of imminent time-based risks, their frequencies and speed of geographic propagation.

Received December 18, 2007.

- Risk quantification and mitigation: The qualitative descriptions of threats should be supported by a generic quantitative approach to measure and classify risks in supply chains. Probabilistic approaches based on historical data of process input and output and access control log files support proactive methods to foresee risks and predict the best contingency plan. As a consequence, crises in SCOR-based supply chains can proactively be controlled and losses can be minimized.

The remainder of this paper is organized as follows: In section 2 the state of the art gives a brief overview of supply chain models focusing on risk management and security concerns. Section 3 is devoted to the security in the SCOR model at three different levels. Risk identification and formal approach are presented in section 5. Integrating risk management to SCOR by identifying various sources of threats and risk parameters are discussed in section 6. In section 7 roadmap and benchmark are presented to generate risk assessment plan and define risk best practices. Section 8 presents the conclusion and future work.

2. State of the Art

In the 1980s the term Supply Chain Management (SCM) [3] was developed, to express the need to integrate key business processes, from the end user to original suppliers – the original suppliers being those that provide products, services and information that add value for customers and other stakeholders. The basic idea behind SCM is that companies and corporations involve themselves in a supply chain by exchanging information regarding market fluctuations and production capabilities. There are several varieties of supply chain models, which address the business activities associated with all phases of satisfying a customer's demand: The Value-Chain Group introduced the Value Chain Operations Reference (VCOR) Model [4]. VCOR focuses on three centers of excellence, namely, product excellence, operations excellence, and customer excellence, to create and add value to customers. The Global Supply Chain Forum (GSCF) [5] introduced another Supply Chain Model. This framework consists of eight key business processes. Each process is managed by a cross-functional team, including representatives from logistics, production, purchasing, finance, marketing and research and development. The SCOR (Supply Chain Operations Reference) model, developed by the Supply Chain Council [6], measures total supply chain performance. SCOR becomes a process reference model for supply-chain management. It includes delivery and order fulfillment performance, production flexibility, warranty and returns processing costs, inventory, and other factors in evaluating the overall effective performance of a supply chain. Unfortunately risk indicators are not considered in these models. A few works have studied the integration of Risk Management in supply chain management [7, 8, 9, 30]. Authors in [8] have studied the impacts of crisis and mitigations that defect supply chains strategies with product uncertainties. The PROTIVITI APICS survey [9] and outsourcing risks in [31] recognize the impacts of crises on chain organizations.

The integration of risk management is a de facto standard, such as SCOR, is a viable trend to rigorously control and monitor emergence of crises by means of quantitative tools and plans. Security access control and secure data exchange are crucial to reducing risks and maintaining trust relationships among partners and the assurance of the quality of shared data in secure supply chains [30].

3. Security in Supply Chains

The SCOR model provides a global approach that links business processes, metrics, best practices and technological features into a unified structure to support communication among supply chain partners. It also improves the effectiveness of supply chain management [2]. Securing this model is essential to creating a cooperative framework and establishing mutual trust relationships between organizations and stakeholders. The security in supply chains involves methodologies for the analysis, design and implementation of security requirements related to data and processes [29].
The SCOR model consists of five interrelated processes (i.e. Plan, Source, Make, Deliver and Return) each of which is presented at three description levels. A process at level 1 is composed of fine-grained processes at level 3. This hierarchy of processes is prone to confusion regarding rights for controlling access to process inputs and outputs. The security of exchanged data, contextual and collaborative processes and network communication expose supply chains to risks.
We hereafter introduce security concerns in supply chains through two-dimensional flows of information to control access to data of input and output processes: The vertical flow of information between SCOR process levels concerns the security policies inside the firm. Vertical security focuses on credentials needed by chain actors by defining role-based access control within each firm. The horizontal flow of information deals with trust relationships between customers, suppliers and stakeholders, and securing the content of exchange data and communication protocols.

We limit our study of the security in the SCOR model to 3 levels. Based on the flow of information in each level, we identify three different classes of roles related to data management: Senior management, middle management and operational management as illustrated in Figure 1.

Figure 1. Classes of Roles and Vertical Flow of Data Management

The supply chain can be considered as a cooperative model or extended workflow across firms [30] handling data access controls and process constraints. Workflow systems often grant access to users of resources by means of processes.

Trust responsibilities and roles should be considered in the design of security policies and risk evaluations. Workflows are process-centric in general whereas security policies are user-centric systems controlling access to resources (i.e. databases). Managing risks due to security should take into account the following source of threats in a context of supply chains [30]:

1-Authentication: A SCOR-based supply chain defines different domains of access to processes and their activities. Actors identify themselves based on their roles. Since the concept of activity-domain is already defined in the SCOR model, the generalization of this concept can be extended to denote Process Domains (Planning, Source, Make, Deliver and Return) to gain access to various processes at different levels by the authentication mechanism [30]. Actors that have to interact with different process domains need to have different roles assigned to each process domain. For example, a senior supply chain manager may have rights to access input and output data of the PLAN process and its sub-processes whereas an operator may only have rights access MAKE process.

2-Authorization: Supply chain participants in SCOR are authorized to undertake particular functions or operations. The role concept defines a set of operations that authorized participants can do such as Start a process, Close a process, Stop a process, Resume a process, etc. The access control is the mechanism by which actors are allowed to access domains according to their identities (i.e. authentication) and operate with respect to their associated privileges (authorization).

3-Auditing: The audit activity consists of maintaining the history of system events and operations across the supply chain and enabling the subsequent identification of relevant events to security attacks and failures. Auditing concerns in particular data related to SCOR process inputs and outputs.

Including security concerns in the management of risk makes the contingency plan efficient to deal with real world risks and crises of the context of SCOR-based supply chain. Despite initiatives of the supply chain community to propose reference models and integrate risk management these efforts do not take into account risk-failure and security policies to monitor processes and provide decision support.

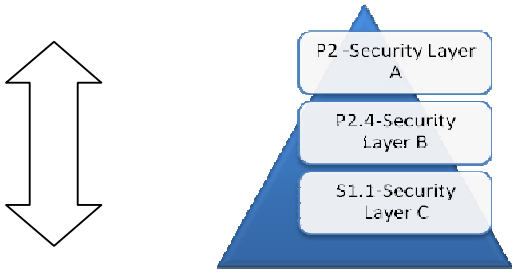

Figure 2. A Snapshot of Security Classifications of P2.4 SCOR Process and Sub-Processes

Layer A	Layer B	Layer C
P_2	$P_{2.4}$	$S_{1.1}$, $S_{2.1}$, $S_{3.1}$, $S3_{.3}$, $ES.3$, $ES._4$

Table 1. Output of the P2.4 SCOR Process

We propose a segregation method to classify SCOR process security levels depending on process domains and roles. The security classification differs depending on the level of the decision or level in which an action is taken. The security layers in Figure 2 define for each process in SCOR an executive level. The class "A," for example, identifies a security level where all actors belonging to the senior management have similar profiles and security schema, and can execute common operations. By using the definition of the "ABC" classification of security levels, risk assessment and monitoring can be easily defined.

Conversely, the horizontal flow of information to establish trust relationships allows the SCOR model to act as a mediator between SCOR-based supply chains (see Figure 3). At this stage, security levels should define process domains with respect to authentication, data integrity, data privacy and auditing.

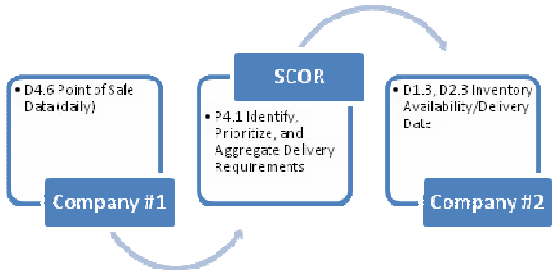

Figure 3. Horizontal Information Flow and Trust Relationships

4. Risk Impacts

Risk Management is an attempt to minimize the chances of failure caused by unplanned events or planned events. Organizations of all sizes have recognized the need to put strategies and capabilities in place in order to identify, prioritize and manage risks as well as opportunities across their entire supply chain and also within and across their internal supply chain processes.

Crisis or Risk Management is applied to companies which directly control their decision making process and when the crisis is not devastating. Although disasters cannot to be controlled from spreading, their impacts and side effects can be minimized throughout the supply chain.

For some industries, supply chain performance can be a real competitive differentiator [8]. Therefore managing risks becomes a prerequisite for success or even survival. For example, procurement services have many risks. Contract management and purchasing execution also have many risks, etc. These areas of risk include [9]:

Supply interruption risks
Demand and supply planning and integration risks
Purchase price risks
Inventory and obsolescence risks
Customer satisfaction and service risks
Process inefficiency risks
Human resource skills and qualifications risks

Project management risks
Information integrity and availability risks

Risk Management is not a management of surprises it is a rigorous decision making process that is affected by three factors, the risk subject, the time/duration, and the Impact.

Proactive prevention of crises consists in advanced planning and necessarily takes measures to build a protection roadmap and an alert plan before a crisis happens. Because of uncertainties in supply chain management, simulation tools are of great help to forecast future crises. The crisis intensity diminishes when it is expected plan in advance.

Various business firms in the same sector of activities have different characteristics and thus what is risky for one firm might not be for another in the same sector. This dependency relies also on the risk reflex and the proactive managerial skills of each firm.

The environment also has a major effect on risks, the crisis reflex of managers and risk intensity. A manager in an African rubber company might not have the same risk reflex as a manager in a Canadian rubber company, due to different circumstances, geographical locations, and market economies. As a result, Risk Management is unique between these companies in the same sector whereas the rubber prices are affected worldwide. Both companies are directly affected by a different intensity depending on their risk, crisis management and planning.

The scarcity of resources and time constraints lead to the attribution of a priority rating for each risk, taking into account existing activities, processes or plans that operate to reduce or control the risk, deliveries and timing.

The significance of a risk can be expressed as a combination of its consequences or impacts on a process's objectives and outputs, and the likelihood of those consequences arising (Impact and Likelihood).

This combination can sometimes be accomplished with a matrix defining the significance of various combinations. Table 2 illustrates the general principle contained in most priority-setting processes: risks are high-priority if problems are likely to arise and if they have large potential consequences. In Table 2 the basic priority-setting matrix demonstrates a simple assessment [1].

Likelihood	***Consequences***				
	Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Almost certain	M	M	H	H	H
Likely	L	M	M	H	H
Possible	L	M	M	M	H
Unlikely	L	L	M	M	H
Rare	L	L	L	M	M

Legends: L = Low, M = Medium, H = High

Table 2: Impact and Likelihood Combinations

5. Quantifying the Risk Exposure

Risk identification generates a list of risk items that might impact the supply chain project and its processes. Often the list is extensive. The risk assessment consists of separating the important items from the less important ones. Risk assessment has several objectives:

-Give an overview of the general level and pattern of risks related to the project and processes;

-Stress on the high-risk items ;

-Help to decide immediate action/decision and whether an action plan should be developed.

-Facilitate the allocation of resources to support management's action and decisions.

An analysis phase of risks allows for the identification of classes of risks and the support for appropriate actions. Three types of analyses can be useful to carry out risk assessment.

• Qualitative analysis [1] is based on nominal or descriptive scales for describing the probability of occurrence or, probability of occurrence and consequences of risks. This is particularly useful for an initial review or screening or when a quick assessment is required.

• Semi-quantitative analysis [1] extends the qualitative analysis process by allocating numerical values to descriptive scales. The numbers are then used to derive quantitative risk factors.

• Quantitative analysis [1] uses numerical ratio scales for probability of occurrence and consequences, rather than descriptive scales.

Based on quantitative analysis, we use the "Calculated Risk," a simple arithmetic formula, to classify risks. The Calculated Risk refers to the risk that a firm can handle or the cost it is willing to support in case it happens. The Calculated Risk is formerly expressed by the risk exposure as follows:

$$\text{Risk Exposure} = (P \times I \times W)$$

Where:

- P denotes the probability of occurrence and it represents the chance that can be subjectively quantified and assigned to the occurrence of a dysfunction/incident per year. This parameter depends on previous experience, the circumstance in the environment and the risk criteria (i.e. business, politic, technology, legal etc. ($0 \leq P \leq 1$) [10]

- I denotes the impact of a risk in order to highlight its effect on the organization. This parameter is important to the normal functioning of a process has one of the following values: 1 (less important), 3 (moderately important) and 5 (very important).

- W denotes the Weight, denotes the importance level an organization can give to a risk. Two companies in the same sector might choose different "W" for a particular risk based on their internal reflex or managerial processes to solve the crisis. The weight can play a determinant role to increase or decrease the risk exposure. This parameter might be on a scale from 0 to 10 as follows:

10 (Extremely important), 8 (Very important),
6 (Very significant), 4 (Significant),
2 (Less significant), 0 (Not Important).

We suggest to map risk exposure values to 3 classes of importance A, B and C, where A is the most important class and C is the less important.

$$0 < C \leq 1;\ 1 < B \leq 5;\ 5 < A \leq 50;$$

For planning assessment all A class Risk Factors must first be solved then the B class Risk Factors and lastly the C class risk factors.

Quantitative risk analysis assigns to each risk a priority rate [1] and takes into account existing activities, processes or plans in order to reduce or control the risk.

In addition to the classification of risks through the ABC classification, we introduce the concept of occurrence risk criteria, called relative frequencies, which is defined in terms of the history of past occurrences of an event. By using this ratio, forecasting the risk becomes more accurate and based on real and not subjective data.

$$P = \sum Past\ Events \div \sum Observations$$

P denotes probability [22] and is computed based on the number of times during which the event occurred in the past among the total number of all observations.

6. SCOR Model and Risk Management

The emergence of supply chains which coordinate organizations, people, activities, information and resources dramatically increases risk crises. The interruption of supply chains has a significant impact on the overall performance. The SCOR model defines generic processes and offers an analysis of metrics, best practices, input and output. The reference model is based on five distinct management processes: Plan, Source, Make, Deliver, and Return. The SCOR model does not attempt to describe every business process or activity. Instead, the SCOR model provides three-levels of process detail. Each level of detail assists a company in defining scope (Level 1), configuring a particular supply chain (Level 2), and defining process element details, including performance attributes (Level 3). Below level 3, companies decompose process elements and start implementing specific supply chain management practices. It is at this stage that companies define practices and risk exposures to achieve a competitive advantage, adapt to changing business conditions and analyze risks and failures.

The management of dynamic constraints and uncertainties in the SCOR reference has a dramatic risk of failure if ill-managed. As the SCOR model is designed to only support supply chains of various complexities across multiple industries, the integration of Risk Management in the reference model becomes a crucial part to enhance the performance, and evaluate risks. Coupling Risk Management and the SCOR management allows for the control of threats and failures while the supply chain is implemented.

6.1 Types of Threats

The examination of information flow between SCOR processes shows that the outputs of one process are the inputs for other processes which might not be fully controlled by the same company or the same manager. The diversity of the business context and cross-organization of processes drive the company to foresee all unpredicted crises. Unfortunately, risks arise at various levels of the supply chain i.e. strategic, tactical or operational levels. Different types of failures can be also triggered by a range of elements including people, processes, technology, business decisions and politics to name a few. A brief survey of these crucial elements will illustrate their impacts on the SCOR model.

People: People as clients, operators, employees and managers play a determinant role at several parts of the supply chain. By such, people face problems related to the human nature including communication problems, respecting deadlines, resisting changes and they are impatient as well. This reality influences the project management of the implementation of a SCOR-based supply chain and the daily management of processes (i.e. Plan, Source, Make, Deliver, and Return) [11].

.

Processes: The design of ad hoc or monolithic processes becomes a source of sometimes unbearable cost due to the efforts to align the information system with the business strategy. This potential risk to the evolution of the supply chain is considered as a major handicap to cross-collaboration. The implementation of processes at level four of the SCOR model should allow for flexibility and adaptability to respond to immediate changes due to the business opportunities and environment. [12]

Technology: The implementation of a SCOR-based supply chain project closely depends on the technological infrastructure and software. The integration of new applications within a legacy platform that supports the supply chain can become a difficult problem. Advanced technologies and lack of standards increase the complexity of supply chains and raise risks.

Business: Business decisions introduce various risks that are difficult to foresee. This type of risk proves easily handled through the use of process indicators and decision support systems.

Politics: Businesses are a mirror of human interaction and large-scale organizations present, by such, many occasions for strife, conflict and power struggles. Risks associated with office politics can be faced with the implementation of contingency plans [13].

Resources: Some resources in supply chains are presented in the SCOR model as inputs and outputs at different levels of various processes. In the case that they unplanned and not properly mitigated in advance they run the risk of harming the progress of tasks or activities. In addition to the resources of the SCOR model when a supply chain project does not get allocated required resources such as people, money, facilities or equipment, the project might fail and affect all actors involved throughout the supply chain.

Miscellaneous: This is a category of risks includes elements associated with a force majeure and that are in results hard to foresee.

6.2 Risk of Failure in SCOR-Based Project

Despite the fact that the SCOR model proposes a unified description of the supply chain and its processes, risks remain omnipresent in joining heterogeneous environments and resources. In addition, we divide Risk Management into two major parts: the first consists in the risks of managing a project in order to implement a SCOR-based supply chain and the second deals with the risks at the input/output level of SCOR processes.

Project management risks are mainly related to the participants involved. By such, those who choose team participants must keep an assessment of risk in mind. The

following factors have an impact on SCOR project management:

1. The Experience of Project Participants
2. Risk of having during the SCOR implementation team members with similar level of authority in the company.
3. The risk of not finding an effective steering committee for SCOR implementation with cross-functional relationship. i.e.: team member that have authority not only on the vertical level but the horizontal as well.
4. The risk to not find a team that is knowledgeable and has history in the organization but also willing to learn something new and not resisting the change.
5. The risk of bad attitude of the team members which will lead the project to a direct failure.

6.3 SCOR Risk Mitigation Plan

According to these types of threats as well as the risks of SCOR-based project management, risks of failure are also related to each level of SCOR supply chain processes. Risks might possibly have side effects on the input and output of all processes in which the flow of information might fall out of sync with physical goods whereas all of these processes should work simultaneously. Based on this scheme and from the Risk Management perspective, every input and output in each process must be studied and controlled in order to manage expectations and deliveries at each stage of the supply chain.

By analyzing threats throughout all SCOR processes, risk assessment identifies risks for each input and output. A list of potential risks and their appropriate mitigation plans are attached to the studied process. Risk exposure is also calculated to classify its level (i.e. A, B or C).

To overcome risks an eventual Mitigation Plan should include the following tasks:

-Planning for crisis intervention and mitigating the risk.

-Gathering information about how similar situations were faced and solved.

-Building a scoring schema to be able to select what is important and prioritize the treatment.

This Risk based management can be implemented at any level in SCOR, the Risk exposure formula, its mitigation and plan are all generic to any level.

Based on the SCOR documentation of level 3 processes, the Figure 1 illustrates the flow plan of the Delivered Stored Product Process (D1.3) and its tasks. The risk classification of each input and output demonstrates the significance and priority of an eventual mitigation.

6.4 Risk Perimeter in SCOR

Risk management is comprised of strategic and operational risks [25]. Processes in SCOR are directly involved with strategic decisions. By such, their related risks must focus on operational risks whereas the risk related to the choice of suppliers is considered strategic and often irreversible in the sense that the cancellation of an action proves costly in resources and money. In addition, the flow of information, inputs and outputs of processes are interrelated in SCOR-based supply chains. In particular, the information flow can reach suppliers, suppliers' suppliers, customers, customers' customers and so on. At the same time, the information flow links different departments in the same firm. The information flow characterizes internal and external risks [23] based the firm's boundary. The internal risk is usually managed by the firm and caused by process inputs and outputs within the information system. What is considered an internal risk can be corrected and maintained in-house (see Figure 4). The external risk is related to process inputs and outputs connected to partners' information systems (i.e. customers, suppliers, governmental administrators, stakeholders, etc…) by means of the supply chain.

Depending on risk perimeters, SCOR risk analyzers have to follow different plans to manage risks and quantify their exposure. Internal risks are almost controlled and predictable since they are directly related to the firm culture, worker skills, technical problems, management and so on. External risk factors are more difficult to control due to supply chain complexity including uncertainties, external decision making processes, frequency of occurrences and time exposure. In this case, SCOR risk analyzers do not easily manage risks nor minimize their impacts.

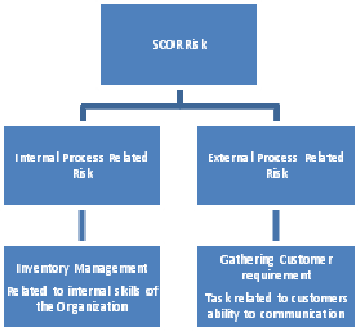

Figure 4: Internal and External Risks

Previous research has been carried out on this topic to differentiate between risk and uncertainties [25]. To successfully manage risks in an environment of uncertainty risk assumptions must be set in order and use probabilistical criteria (i.e. Hurwicz, Wald, Savage and the Laplace criterion) [24, 27].

6.5 Time and Space Based Risks

Due to uncertainties, risk prediction becomes more difficult when the crisis date is not known. In this case, time factors directly affect the decision making process and risk reflex of decision makers. Analyzers tend to predict risks that are likely to occur in the short term rather than focusing on risks that might occur with a delay in the unknown future. As abovementioned, historical occurrences of crises are also a major indicator of what might be the future of any process. SCOR risk management has to consider time factors so that management will be able to use its resources in an appropriate manner by investing necessary means. Overseeing all risky processes at the same time is in of itself risky [25]. For most projects,, the factor of time, a payback period and Internal Rate of Return (IRR) are used to compute the financial cost of efforts that should be invested to carry out projects. These financial indicators affect the priorities of risk mitigation. The organization of supply chains is dynamic and evolves over time and geographical locations. Risks can propagate through the supply chain which should take into account the forecasting of imminent time-based risks, their frequencies and speed of geographic propagation.

7. Risk Roadmap and Benchmark

The qualitative descriptions of threats and SCOR-based project management risks should be completed with a generic quantitative approach to measure and classify risks. This approach, which is based on risk exposure, includes:
- A Risk Roadmap to build for each SCOR process.
- A Risk Benchmark framework as part of a Risk Assessment Plan.

7.1 Risk Roadmap

The risk roadmap is the output of an exhaustive process analysis which focuses on Strengths, Weaknesses, Opportunities and Threats (SWOT). The roadmap identifies risk list necessary changes to apply to SCOR processes in order to control risks. For each potential risk list related to input or output of a process an appropriate contingency plan is defined. The roadmap includes the following parts:
1- Define the weight of each risk.
2- Define risk exposure and their levels of importance.
3- Estimate the time needed to execute the appropriate contingency plan.
4- Define the Return On Investment (ROI) and assess the validity of the mitigation plan.
5- Reduce to zero the occurrence of similar risks.
6- Capitalize on experience to solve similar situation in the future [14].

The roadmap of the SWOT analysis provides a strategic and operational document allowing to compare the current state of a process (i.e. actual plan) and its pre-planned risk-free state (initial plan). An accurate Monitoring Process based on the roadmap alerts drive processes and identifies the need to re-organize business processes to reduce risk occurrences

These alerts are based on KPI (key process indicators) coupled with an accurate monitoring process to control any deviation from the foreseen plan using. The KPIs are specific to each organization and can be easily quantified and controlled through the information systems in the organization [15].
Based on Key Process Indicators (i.e. time, quantity produced, money invested, etc.) the management monitor each process alongside the desired plan and set triggers on the KPI to launch alarms integrated in the Supply Chain Information systems and Decision Support System [16].
This part will play a major role in the real-time simulation process where each KPI have a major role into building assumptions criteria [17].

For example, if the success of the supply chain means the maintenance of a certain threshold of stock, for example, up to three months of consumption, and if the SWOT analysis reveals that risk exposure in this process is “High,” then the procurement process and the consumption process should be carefully monitored in order to guarantee three months of stock capacity. In this case, the safety stock is a strategic success factor in the SCOR process.
The SCOR model defines five critical success factors to deal with supply chain performance; delivery reliability, order flexibility and responsiveness, supply chain cost, and effective asset management [18]. Unfortunately, these factors require ready contingency plans to deploy and to overcome crises. We introduce a new success factor, called risk control and crises management factor that aims to make the supply chain’s performance hazardless.
As a result, the roadmap which supports the risk control and crises management factor takes into account critical SCOR success factors to establish the list of risks. Critical business factors that emerge from threats are also considered to enrich the list of risks. For example, if technology is negatively impacting sales, if market penetration is very slow or, if inventory is not being 100% controlled.

7.2 Risk Benchmark

In addition to the definition of the risk control and crises management success factor, the SCOR model can improve its generic process definitions with Risk Best Practices in a similar way to best practices of its processes. Risk Best Practices as problem-solving patterns of various risks help to establish contingency plans and provide the best solutions for specific risks and crises [19].

Based on Risk Best Practices a Risk Benchmark of supply chains will evaluate risks due to common practices by comparing them against Risk Best Practices and provide proactive risks policies. Monitoring prior performance and mitigating risks and crises drive supply chains to strive for excellence and quality. Another interesting application of the benchmark includes the simulation of the Risk Plan [20]. Whenever a crisis occurs the estimated time to solve the problem becomes a crucial parameter. The aim of risk simulation is comprised of the following steps:
1- Minimize the response time.
2- Develop the team’s awareness to manage priorities.
3- Update the knowledge base of risk best practices and maintain an accurate Risk Plan.
4- Adjust the project schedule in a flexible manner to respect deadlines and delivery constraints.

In Table 3 what would happen if, for example, the P2.4 Sourcing Plan is defected? Are the appropriate Risk Plan and the risk class priority easily controlled and can the crisis be easily encountered? In case the Risk Plan is not defined, a risk awareness attitude should be developed by simulation, for example, periodic triggers of false threats can build confidence and offensive attitudes in firms towards crisis and accordingly adjust attitudes and decisions to deal with real crises whenever they happen.

Table 3 A Snapshot Classification Template Risk Exposure of the D.1.3 SCOR Process

Task D.1.3	*Description*	*Risk*	*Mitigation*	*P*	*I*	*W*	*RE*	*Risk Class*
			Input					
P2.4	*Sourcing Plans*	*Supplier is unable to deliver on time because of IT troubles*	*Blanket purchase orders covers period requirements*	*0.5*	*5*	*5*	*12.5*	*A*
P3.4	*Productions Plans*	*Might create a bottle neck in the production line*	*Keep production lines ready for unplanned orders in order not to impact the product delivery plan*	*0.1*	*5*	*5*	*2.5*	*B*
P4.4	*Deliver Plans*	*Plans might not be accurate*	*Keep an acceptable margin and safety zone*	*1*	*3*	*5*	*15*	*A*
S	*Inventory Availability*							
M								
M1.1	*Production Schedule*							
			Output					
P1.1	*Order Back Log*							
P4.1								
P4.2	*Inventory availability Delivery Date*	*The process of identifying, evaluating, and considering all things that add value in the delivery of a product or service.*	*Key persons expertise is not up to the level to give such an accurate evaluation*					
P, S, M, D	*Inventory Status*							
S1.1	*Replenishment Signal*							

8. Conclusion

Nowadays, risk and crises in firms increase due to uncertainties, a lack of security, scarcity of resources, and a range of factors including people, processes, technology, business decisions and politics [21]. This turbulent environment requires firms to be proactive and rethink their Supply Chain models and business processes. Building a risk-based, secured management for Supply Chains, managing risk and controlling the impact of crises, might all be good ideas to enlarge and improve the SCOR-based supply chains. In this paper we present a generic framework to extend the SCOR model by the integration of the risk management discipline to supply chains. This framework attempts to identify potential categories of threats and their impacts on managing processes. In this context, we take into consideration the security, in particular, the access control to enhance the risk assessment plan. We discuss different qualitative and quantitative approaches to classify risks. As the SCOR model defines generic processes and offers an analysis of metrics, best practices, input and output, we study types of threats triggered by a range of elements including people, processes, technology, business decisions and politics to name a few. Depending on internal and external risks we propose to follow different plans to manage risks and quantify their exposures by analyzing threats throughout all SCOR processes. We also introduce a generic quantitative approach to measure and classify risks including Risk Roadmap and Risk Benchmark, to build for each SCOR process.

Future work is destined to consider the creating of a risk benchmarking database where a risk knowledge management system can be implemented to simulate large scale SCOR-based supply chains.

References

[1] D F. Cooper, S Grey, G Raymond and P Walker. Project Risk Management Guidelines, John Wiley and Sons Ltd, 2005.

[2] Supply Chain Council, Supply Chain Operation Reference (SCOR) Version 9.0, [Website http://www.supply-chain.org], last visited April 2009

[3] S. Chopra, P. Meindl, Supply Chain Management, Strategy, Planning & Operation, Third Edition, Pearson Prentice Hall, 2001.

[4] Value Chain Group, Business Process Transformation Framework [Website http://www.value-chain.org/] Last visited April 2009

[5] D M. Lambert, Global Supply Chain Forum, [Website http://www.fisher.osu.edu/centers/scm/], Last Visited June 2007.

[6] D. Stauffer, Risk: The Weak Link in Your Supply Chain, Harvard Management Update Article, 2003.

[7] H L. Lee, Aligning Supply Chain Strategies with Product Uncertainties, California Management Review, Vol. 44, No. 3, 2002.

[8] P. O'Keeffe, Understanding Supply Chain Risk Areas, Solutions, and Plans, Protiviti and APICS Study, ROTIVITI independent Risk Consulting - 2004.

[9] D N. Chorafas, Integrating ERP, CRM, Supply Chain Management, and Smart Materials, Taylor & Francis Ltd, May 2001,

[10] B. Wahlstrom, Models, Modeling and Modelers: an Application to Risk Analysis, European Journal of Operational Research, Vol. 75, No. 3, pp. 477-487, 1994

[11] P. Thomson, Engineering Construction Risk, A guide to Project Risk Analysis and Risk Management, London, Thomson Telford, 1992.

[12] Y. Papadakis, Operations Risk & Supply Chain Design, An Event Study, LeBow College of Business, Drexel University, USA, 2002.

[13] R L. Kleim and Irwin S. Ludin, Project Management Practitioner's Handbook, AMACOM Books, 1998.

[14] T L. Barton, William G. Shenkir, P L. Walker, Making Enterprise Risk Management Pay Off: How Leading Companies Implement Risk Management- Financial Times Prentice Hall, 272 pages, 2002.
[15] M. Dalal, B. Groel, A. Prieditis, Real-Time Decision Making Using Simulation, Look Ahead Decisions Inc. Proceedings of the 2003 Winter Simulation Conference, pp 1456 – 1464, Vol.2, 2003.
[16] K. Laudon and J. Laudon, Management Information Systems Managing, the Digital Firm, Prentice Hall, 10th Edition, pp.736, 20087.
[17] J. Bermudez, Supply Chain Management: More Than Just Technology, March/April issue of Supply Chain Management Review, 2002.
[18] J. Francis, Team Building with the Supply-Chain Operations Reference Model, March issue, Supply Chain Management Review, 2007.
[19] P. Bolstorff, R. Rosenbaum, Supply Chain Excellence — A Handbook for Dramatic Improvement Using the SCOR Model –AMACOM Press, pp 256, 2003.
[20] DR. Dimitris N. Chorafas, Integrating ERP, CRM, Supply Chain Management, and Smart Materials, Auerbach, Press, pp. 408, 2001.
[21] M. Fayez, L. Rabelo and M. Mollaghasemi. Anthologies for Supply Chain Simulation, University of Central Florida, 2002.
[22] D. Lind, W. Marchal, S. Wathen,. Statistical Techniques in Business and Economics,10th edition, McGrawHill, pp. 147, 2005.
[23] J.H.M Tah and V. Carr, Toward a Framework for Project Risk Knowledge Management in Construction Supply Chain, Advances in Engineering Software, Elsevier Science Ltd, pp. 835 – 846, 2001.
[24] L. Neuman, Quantitative Approaches to Management, 5th Edition, Allyn & Bacon, pp. 592, 2002.
[25] H. Kerzner, Project Management: A System Approach to Planning, Scheduling, and Controlling, Wiley Publishers, 9th Edition pp. 1040, 2006.
[26] T. Luckey and J. Philips, Software Project Management, Wiley Publishing, pp. 309, 2006.
[27] F. Reilly and K. Brown, Investment Analysis and Portfolio Management, South-Western College Publishers, 8th Edition, Wiley, pp. 1200, 2008.
[28] R. Neapolitan, Learning Bayesian Networks, Northeastern Illinois University Chicago, Illinois, Prentice Hall, pp. 674, 2003.
[29] R. Azari, Current Security Management & Ethical Issues of Information Technology, Hershey, PA: Idea Group Publishing, 2003.
[30] WfMC, The Workflow Management Coalition Workflow Security Considerations, White Paper, Document Number WFMC-TC-1019, 1998.
[31] N. Benvenuto and D. Brand, Outsourcing—A Risk Management Perspective, Information Systems control Journal, Volume 5, 2005.

Author Biographies

Dr. Youakim Badr received a Doctorate in Information Systems from the French National Institute for Applied Sciences in Lyon (INSA of Lyon). He joined the faculty of the INSA of Lyon as Associate Professor of Computer Science in 2003. Dr. Badr has worked extensively in the field of Productions Systems, Virtual Enterprises and e-commerce. His current academic research interests include systems in both the service sector and ICT. In particular, he studies the ecosystem of services and the multidisciplinary modeling approach to design services through the integration of ICT, strategy and processes. He leads the Service-Oriented Enterprise research team which combines industrial and computer engineering approaches. Dr. Badr is vigorously involved in a series of international conferences and serves as a reviewer for various conferences and journals.

Jean S. Stephan received a Master degree in Computer Science from the University of Lyon II, France in 1993, a MBA degree from the Lebanese American University, Beirut, Lebanon in 2003, and a Master degree in Management from Saint Joseph University, Beirut, Lebanon in 1990. Since 1996, he has been working on Information Systems and ERPs implementations. At present, he is a lecturer in Saint-Esprit University, Kaslik and Lebanese American University (LAU) Beirut, Lebanon. His major fields of study include information systems, supply chains, and risk management.