Resilience and Outsourcing

Bernardo Nicoletti

Abstract

Today's social-economic environment is turbulent and uncertain. The turbulence has tended to increase for a number of reasons. Demand in almost every industrial sector seems to be more volatile than was the case in the past. Product and technology life-cycles have much shortened. Competitive product introductions make life-cycle demand difficult to predict. At the same time, the vulnerability of the organizations to disturbance or disruption has increased. It is not only the effect of external events such as atmospheric events, strikes or terrorist attacks, but also the impact of changes in business strategy or war and terrorism. Many organizations have experienced a change in their risk profile as a result of changes in their business models, for example, the adoption of 'lean' practices, the move to outsourcing and a general tendency to aim at vendor consolidation. This paper suggests that one key element in any outsourcing strategy designed to mitigate operational risks is improved resilience. The paper analyze how to improve and manage resilience

Keywords: Procurement, Resilience, Outsourcing, Risk Management, Disruptions

Introduction

The environment is more and more turbulent and difficult to predict. On the other hand, more and more organizations use outside vendors to do their functions and processes also essential to their operations. The motivations are simple:

- Add value to the customer;
- Focus on the organization's core business;
- Gain in flexibility.

An interesting case is represented by outsourcing. This term refers to organizations that use external vendors to run their processes or sub-processes. For instance, organizations could outsource the management of a data center, the maintenance of computer applications, or similar. In recent years, there is an increasing interest in this business model. This is the move from one vertical enterprise to a highly integrated system of networked enterprises

In this situation, it is necessary to consider the risks that an organization may incur. One can cite extreme examples from this point of view. Think of what has happened in many organizations as a result of the disaster of the nuclear power plant in Fukushima. Many organizations have lost their supplies for a long time. Or consider the case of hard drives for personal computers. A disaster in a factory in Thailand has reduced dramatically the availability of the components for these products.

Much has been written and said on risks. It is interesting to examine how to protect an organization from such risks. The risks can be of a very different nature. This paper focuses on operational risks. In the so-called Basel Accord for financial services, the operational risks are defined as the risk of losses due to inadequacy or failures of processes, human resources and internal systems, or from external events. This paper examines how procurement can help in the management of these operational risks associated with outsourcing. From this point of view the resilience is a very important aspect to consider.

Literature

Several papers have in the past underlined the importance of resilience mainly in the case of physical supply chains.

Carrozzi (2009) underlined that the provision of basic services such as energy, transport, healthcare, occurs through complex infrastructures in which the methods of procurement and the organization play a key role. These aspects, if not governed properly, due to the occurrence of events of varying severity and origin, can cause instability in the provision of services. The possible consequences can have a high or very high impact on the organizations and, in some cases, to the entire community. Carrozzi's paper highlights the key drivers and procurement Best Practices for proper government of continuity and maintaining service levels of critical infrastructure, with specific reference to the protection of critical information infrastructure.

Turner et al. (2015) underlined the importance of resilience in in project (risk) management. They analyzed answers to questions such as what should be considered beyond the risk horizon, how to interpret those entities that cannot be quantified or qualified with confidence, how to prepare better for the effects of what it is not known. This paper analyzes how to contain the unknown in a timelier and appropriate manner. The paper described what practices can be defined to reach a state of true, although never perfect, resilience. These practices should allow one to deal with risk, uncertainty and complexity effectively.

The aim of the collection of articles presented in the issue of the Technology Innovation Management Review (2015) is to highlight the significance of resilience and develop a shared understanding of the definition, theory, and managerial implications of cyber-risk and cyber resilience in supply chains. In doing so, this collection of articles issue seeks to develop an agenda for future research that provides solutions to the challenges aims to develop a supply chain cyber-resilience strategy, the tools and methods to respond to cyber-breaches in the supply chain, and present case studies of best practice.

Pereira et al. (2014) in their paper have the purpose to understand the role of procurement in identifying and managing the intra- and inter-organizational issues which impact supply chain resilience. Achieving resilience along the supply chain in today's turbulent business environment requires efforts from both internal and external elements of the extended enterprise. This study revealed that procurement activities do make a significant contribution to creating supply chain resilience. Emerging from the literature review, certain intra- and inter-organizational issues were identified that could

impact supply chain resilience. Also the possible actions that procurement could take to enable the enhancement of supply chain resilience were identified. The originality of this paper lies in the identification of intra- and inter-organizational issues from a procurement perspective specifically as they relate to improving supply chain resilience.

Waters (2007) shows that a key principle is that the design of a supply chain has a fundamental effect on the inherent risk, so managers should work together to design resilient chains. A number of standard principles apply to the design of resilient supply chains, such as starting within individual organizations, taking a strategic view, really understanding the concept of supply chain risk, designing chains with risk in mind, always looking for collaborative solutions, and so on. All supply chains vary in detail, but there are some common features of resilient chains. Some of these are essentially physical features, with a resilient supply chain being short, wide and agile, with spare capacity, and so on. Other features refer to relationships, with a resilient chain having collaboration, confidence in partners, visibility, process integration, and so on, to allow a joint solution of mutual problems. Even the best risk management has unexpected events, and when these are severe they are generally described as crises or disasters. The way of dealing with these is to design emergency plans that can be used to deal with any crisis.

All these papers raise deep questions on the role of procurement in creating resilience, which has not been well-explored in the current literature. Not only, but most of these papers concentrate on the resilience of a physical supply chain, while this paper will concentrate on the resilience of the outsourcing from the point of view of the procurement. The subject is relevant due to the increased diffusion of such organizations. For instance, Bovaird (2016) explores recent experience with outsourcing of public services. He highlights how approaches to outsourcing have evolved during the past 30 years, moving through phases of competitive tendering, partnership working, strategic commissioning, prime contracting and, more recently, insourcing. The paper finishes with 10 lessons for commissioners and service vendors that can be used. Unfortunately, none of these lessons deals with how to contract and manage resilience, especially through a proper procurement.

Outsourcing has several risks. Despite the growth of Information and Communication Technology (ICT) Systems outsourcing in recent years, this trend is still the object of strong criticism. A paper has its aim to show the main risks computer outsourcing entails in the case of the largest Spanish organizations (Gonzales et al., 2005). The Authors analyzed the results of a survey hat was answered by 357 organizations. The main concern with ICT outsourcing is the excessive dependence on the vendor which this type of contract can generate. Nevertheless, some characteristics of organizations (mainly their size) find that to some extent what risks are seen as the most relevant. The conclusions also suggest that full outsourcing could turn out to be a very risky strategy, mainly due to the dependence it creates.

Outsourcing the information processing activities is a complex issue that entails considerable implications for the procurement of an organization (An important mechanism for managing the performance of outsourcing vendors is incentive contracts. But to develop an outsourcing contract the ICT managers must quantify risks

and benefits. Methods and tools for analyzing and quantifying outsourcing risks that ICT managers have at their disposal are rudimentary. A paper by Osei-Bryson et al., (2006) presents a method and some mathematical models for analyzing risks and constructing incentive contracts for ICT outsourcing.

There are relative few studies on how to manage the risks in general outsourcing (Sullivan et al., 2005). This paper stresses the importance of resilience in outsourcing and the way to manage it.

Agility

In general, resilience refers to the ability of a material to deform elastically, to bend opposite to a stress without becoming distorted permanently. This is exactly what organizations need to meet the growing challenges of socio-economic environments. Resilience in the case of outsourcing is the ability of a service provided by an outsourcer to adapt to the conditions of use and to resist external events so as to ensure the availability of the services to be provided.

All the previous characteristics of resilience can be summarized in one word: agility of the organizations. This is the basic characteristics for increasing the flexibility of an organization to deal with unexpected events (Waters, D., 2011).

Risk is based on uncertainty. It exists in all operations. So despite the best plans organizations are always susceptible to unforeseeable events. They must have the flexibility to deal with them. The best way to increase flexibility is to have an agile organization. Agility means that operations are flexible enough to deal effectively, efficiently, and economically with rapidly changing conditions. For instance, rather than increasing the number of resources for creating an outsourcing capable of dealing with unexpectedly high demand, an organization can use flexible operations to increase deployment and deliver services with short lead times. In practice, it is often difficult to predict the details of events that might follow risks, so agility is often the best response.

This can be achieved in several ways, such as: Short lead times, so that all changes are completed fast, making it possible to recover quickly from disruptions. Standardization can help very much. Standardized processes, the same sub-processes used in different outsourcing operations, cut down on resources, delivery problems, work in progress, number of vendors, and so on. The important point for agility is that operations can switch from one service to another without waiting for deliveries of new resources. Standardized operations for different processes so that they can switch seamlessly between products, with cross-trained employees moving to areas of shortage. Rapid rescheduling of operations, diverting work and resources away from areas of surplus and towards areas with shortages. Moving operations between different locations when the risks to one place increase, for example perhaps moving processing from one data center to another, as is possible with cloud computing. Concurrent development to speed up new methods and products. Flexible vendors, using multiple sources with different features to meet differing needs, different kinds of contract, and spot markets.

Studies on the effect of standardization shows there are benefits at least in the case of BPO (Business Process Outsourcing). (Wüllenweber, 2007). A paper aims to give an exploratory first step by suggesting that process standards have a positive impact on business process outsourcing (BPO) risk, Theoretical! Drawings from perceived risk theory and the theory of reasoned action allow one to develop a model of BPO risk. The model empirically shows that risk perception is higher for less standardized processes. Using data from 126 German banks, the paper demonstrates that financial and performance risks are significant different between high- and low-standardized processes. Risks are consistently higher .for low standardized processes.

Resilience and its basic characteristics

Some characteristics are important for ensuring the resilience of outsourcing. They are distinct, but in fact they are quite interconnected. Some authors have considered them in the case of resilience in general (Waters, D., 2011, About Resilience, Gulati, 2013).

This paper will generalize them in the case of outsourcing procurement and refer to them as the nine C's (see also Figure 1):

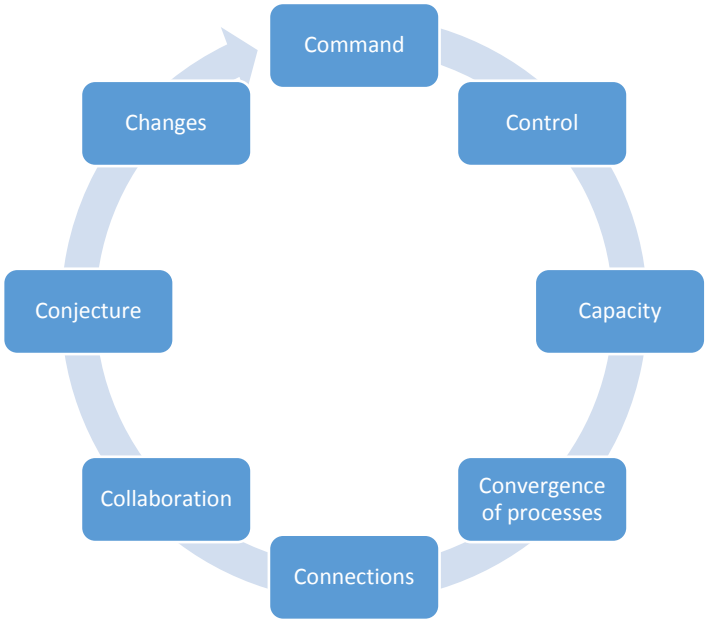

Figure 1 The basic aspects of Resilience

- **Contract**. This characteristic refers either to a contract with a vendor or more precisely to the commitments to the customer for the supply of the service. It is at the base of the other characteristics, which must be clearly spelled out and defined in the contracts.

- **Command**. Command is important for risk management. The organization must have an effective leadership of the outsourcing, both internally and on the vendor side. The leadership must be able to make decisions before, during, and after a

disaster. It must be also efficient, and therefore able to intervene with timeliness, and economics. The risks and the potential disasters must be managed taking into account the objectives of profitability of the organization.

- **Control.** Control is connected with the ability of having a sound governance of the outsourcing. It implies a strong and detailed plan. It must also take into account the imponderables. It must include the "what if" and then take into account and consider the management of what might happen.

- **Conjecture**. Conjecture implies the capacity to forecast or anticipate the occurrence of a disaster. It is important to consider risks in the design. Prevention is better than cure (Michaels, 1996). To be more specific, the best options for mitigation (in descending order of preference) are based on trying to prevent a harmful event from happening, then reducing the consequences if it does happen, and finally seeking redress for damage after it has happened. The customers and outsourcers should explicitly include the effects of risks in their decisions. If they ignore risk, they will focus on leanness, efficiency or some other goals that inadvertently increase vulnerability. The best design needs a balance between resilience and normal measures of efficiency. For instance, a single path through any activity in the process creates a vulnerable point. If anything happens at this point the whole process is at risk. The way to avoid such risks is possibly to design a process with parallel paths. In this way, flows can be diverted away from a disrupted path to one that is working normally. This involves a continuous monitoring of the outsourced services that must be resilient.

- **Capacity**. Very often organizations push on being lean and as a consequence reducing waste, such as overcapacity or quantity of resources. This is fine, but you cannot go overboard in ensuring the resilience and being too lean. It is certainly appropriate to have some extra capacity available in case of emergency.

- **Collaboration.** One of the most important way to ensure a resilient process is through integration, with several members working together to solve mutual problems even if they might belong to different organizations. Without a basic level of cooperation it is almost impossible to make any progress towards a real integrated process. The collaboration can take many forms. It could range from informal discussion to strategic alliances. But the most common forms to share information to increase visibility – with more formal arrangements of collaborative planning, forecasting and resourcing, and synchronized actions. There are various reasons why collaboration is difficult to achieve, but mechanisms do exist and managers have to be persuaded to use them. Sharing information throughout the entire process is the basis of visibility, which means the extent to which one member working on an activity of the process can see what is happening at all points in the flow. This information typically includes demands, seasonality, promotions, new product introductions, industry and market conditions, operations and purchasing schedules, performance, risks, unexpected events, lost sales and any other relevant information. Many aspects

of collaboration in the process can be summarized in 'vendor relationship management'. This is an umbrella term for procedures that allow an organization to cultivate new partners in the process, maintain existing partners, reduce interruptions by spreading business among vendors and locations, and managing risks with sole sources. The sharing of ideas, methods and information is a core part of an outsourcing management. This is the only way that members of the flow can identify mutual risks and design effective ways of dealing with them, gaining synergies from the collaboration.

- **Convergence of processes**. Visibility brings benefits to risk management, but it can also lead to other benefits, including the convergence of operations. In other words, operations tend to converge to common standards and are eventually accepted as the normal way of working. Other initiatives have the same effect, particularly quality assurance and risk management.

- **Connections.** Resilience requires connections flexible but effective, capable of acting in support of events not anticipated. The connections or networks are both from the point of view of computer and telecommunication capacity, in such a manner so as to allow continuity using a back-up if necessary. The connections are also of a business type, with the possibility of resorting to the resources of other organizations in order to allow the continuity in the provision of the services also in emergency conditions.

- **Changes**. Change management requires agility. The agile organization focuses on its "non-negotiable": it is based on creating the right mix of necessary bureaucracy with agility and speed that distinguish the frontline innovators.

The principles of the design of a resilient outsourcing

To analyze the principles of the design of a resilient outsourcing is interesting to follow what is prescribed for supply chain management systems and make the appropriate changes (Waters, D., 2011),).

The design of a resilient outsourcing requires a fully integrated approach (Kleindorfer and Saad, 2005). There are a number of basic principles involved with this move, such as the need for careful design, agile operations, visibility, relationships with customers and vendors, culture, and so on.

Take a strategic view. In common with all major initiatives, Resilience needs commitment from senior managers who are aware of the issues and can allocate the resources. Outsourcing is a strategic initiative that can have deep effects on an organization and the way that it is run. To put it simply, with poor risk management there is less chance that an organization will survive into the long term. But this need for senior support becomes more obvious when it explicitly includes relationships with other organizations, as these inevitably need new strategies and policies.

The first principle in outsourcing resilience is that the basic processes work properly. If the organization which is outsourcing does not have such properly organized processes, the vendor must take the responsibility to make them proper while transitioning in the ambitious move into collaboration. This step makes sure that senior management are committed, they have defined broad policies for risk, a risk management team has been appointed, necessary systems have been installed and tested, there are smooth information flows, an internal risk register has been designed, procedures have been tested, and so on. Only when everything is working internally can managers really expand their scope to consider other members of the chain. An opposing view says that managers can learn valuable lessons from working with others on their joint problems, so they should not approach trading partners with well-defined and inflexible ideas, but should go in a spirit of exploration. The best ideas will emerge from a cooperative approach, combining ideas and experiences so that each can learn new ideas and methods that they can use within their own organizations. Perhaps the best answer is somewhere between these two, where managers make some progress on their own risk management, and then look to improve and consolidate their methods using inputs from other organizations.

The following step is to understand the concept of outsourcing risk. Before they can successfully plan for risk along a process, outsourcers and customers must clearly understand what they are studying. In other words, they must understand the concept of risk – and the members, roles, links, interactions, objectives, forces, dynamics, power and all the other elements that form the complex web of a supply chain. Then they can combine these two concepts in the integrated function of resilience management.

A process is only as strong as its weakest link. Disruption at any point in a process causes problems for the whole flow, so customers and outsourcers have to identify risks throughout the process to find the weakest parts. There are always weak spots in a network, and these might include single paths, links with long lead times, members facing specific organizational risks, those that are unwilling to share information, members that do not manage risks properly, and so on. Sometimes parallel paths can be created around risky areas, but this may be difficult – for example, when there is only one data center. Managers must be especially careful of the risks in vulnerable areas, particularly when these areas are outside their control. Then they might take steps to reduce the consequences of the risk, or try to influence the managers who are responsible by including them in the risk management outsourcing risk management process. Or they can redesign the chain to bypass the area of weakness (Handfield and Nichols, 2002; Kunreuther and Heal, 2004).

The management of an emergency

Resilience requires also an effective, efficient, and economical management of the emergencies. When a risky event occurs, flexible operations can avoid its worst effects and continue to work normally. But sometimes the effects are too severe for even the most flexible operations to deal with. For instance, if a delivery of materials is delayed, flexible operations will allow normal working, but if the supply of materials is completely eliminated, even the most flexible operations cannot find a solution. The alternative is to

build contingency plans for emergencies. These are used as a last resort when all other aspects of risk management have failed, and they work on the basis that, if you do not know what will happen, the best plan is to be prepared for anything.

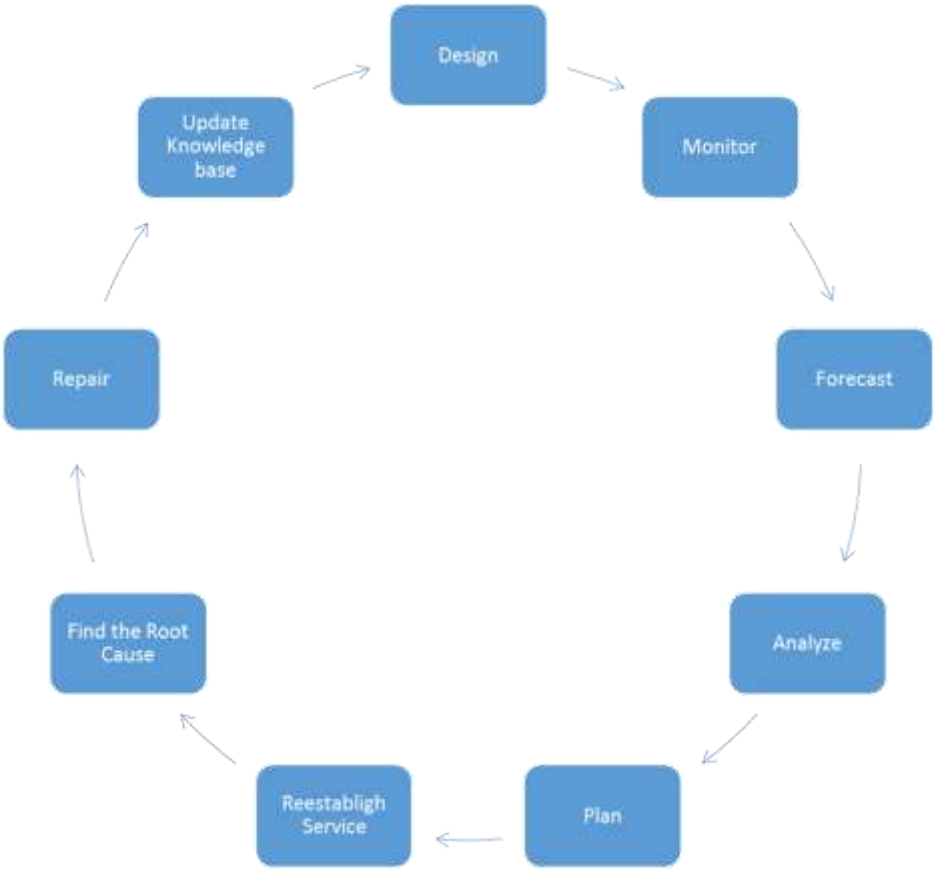

Figure 2: The cycle of risk management

The features of an emergency plans can be represented as in Figure 2. The procurement must request that the service vendor has the capacity along the entire cycle. The vendor must be able to improve its characteristics to manage the risks and the disasters thanks to the buildup over time of its own knowledge base on how to deal with the malfunctions of the outsourced processes and sub-processes.

The first thing to do in case of an emergency is to re-establish the service. Very often this requires to find a workaround rather than solving once and for all the problems. Once applied the workaround, it is necessary to test if it works well or not. If the test is positive one can start resuming the service normally or at a reduced rate.

The following action is particularly important. It is necessary to find the root causes of the incidents. A root cause is a factor that caused a nonconformance and should be permanently eliminated through process improvement (Andersen et al., 2006). Root cause analysis (RCA) is a collective term that describes a wide range of approaches, tools, and techniques used to uncover causes of problems.

Once found the root cause it is necessary to fix permanently the problem. Once done this activity, it is normally possible to fully restore a reliable process. Before applying the fix, as usual it is necessary to test it.

It is important to create and update regularly a knowledge base of all the known incidents and information how to find a workaround and to fix the incidents. This is important in order to improve the resilience of the system in terms of rapid re-establishment in case of known errors. There are many different ways to organize such a knowledge base. One simple but effective way to organize it is as a wiki. This is a website in the intranet or extranet defined in the Encyclopaedia Britannica (see Encyclopaedia Britannica, 2007) which allows collaborative modification of its content and structure directly from the web browser. In a typical wiki, text is written using a simplified markup language (known as "wiki markup"), and often edited with the help of a rich-text editor

The metrics of the resilience

The metrics of KPI (Key Process Indicators) of the resilience must be the measure of the customer satisfaction. Customers are keen in reducing the severity of the occurrence of a risk to both the minimum impact possible and similarly for its duration.

To show graphically what happens in the occurrence of a risk, one can refer to a chart that illustrates how the risks would affect the performance of an organization in terms of sales, production levels, profits, and/or customer service. This paper generalizes what has been introduced as the triangle of resilience (Carvalho et al., 2012) and applies the generalized model to outsourcing procurement. The KPI, which measure the resilience, are shown in what can be called the “graph of resilience” (see figure 3).

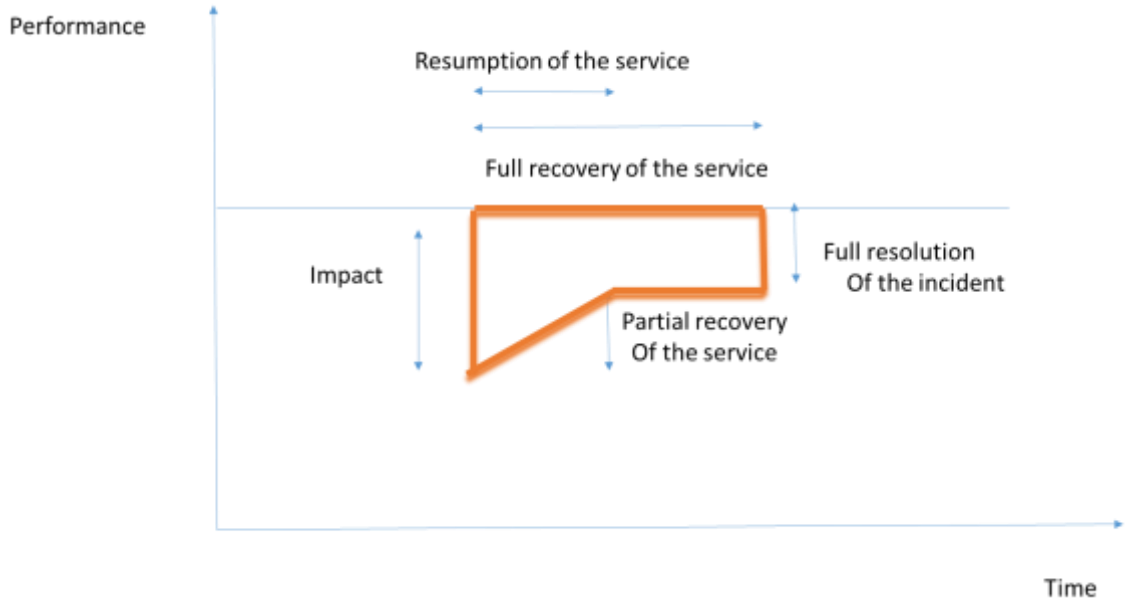

Figure 3: The Graph of Resilience

In addition, the graph shows the different phases of the response system performance: after a risk performance degrades or zero-in. Actions can be undertaken to restore as soon as possible the service (work-arounds). Subsequently it is necessary to identify the root causes and reinstate the performance prescribed in the contracts. These phases can be observed by tracing the organization's response over time as can be illustrated with the "graph of resilience", which displays the scale of the impact and the duration of the negative performance of the outsourced process or sub-process.

The depth of the graph represents the severity interruption, that is, the duration and impact of the damage associated with the disaster. The length of the graph represents the recovery time of the service and the determination and remediation of the root cause.

The graph of resiliency is important for the procurement. Its goal is to negotiate the reduction of the area of the zone in red. To this end, the contract should clearly define the maximum values allowed for the parameters shown in Figure 2 as committed by the outsourcer.

The future

In the future, the outsourcing resilience should be a feature included in all orders and delivery contracts. In fact, it is essential that the resilience be an integral part of the evaluation grid of the potential outsourcing and even better of the potential vendor.

In the case of ICT, products researchers are developing autonomic computing, that is the capacity of a computer system of self-healing or self-unblocking (Montani et al., 2008). This means that it has the capability to autonomously detect failures and recover from them. This property may enable large-scale software systems, aimed at delivering services on a 24*7 fashion, to meet their goals with little or no human intervention. Achieving self-healing requires possibly automatic testing, such as possible with Jenkins continuous integration, and the elicitation and maintenance of domain knowledge in the form of problem determination and diagnosis; repair patterns, a task which can be overwhelming. Case-Based Reasoning (CBR) is a lazy learning paradigm that largely reduces this kind of knowledge acquisition bottleneck (Kolodner, 2014).

Moreover, the application of CBR for failure diagnosis and remediation in software systems appears to be very suitable, as in this domain most errors are re-occurrences of known problems. It is more difficult to develop an autonomic approach in the case of services because of the strong human presence. It is not impossible and very likely the future will reserve some interesting development in this sector.

The more distant future is what is called Digital Resilience. That is the ability to design customer applications, business processes, technology architectures, and cybersecurity defenses with the protection of critical information assets in mind (Kaplan, 2015).

Conclusions

In a situation where organizations depend more and more from outsourcing service vendors, it is a fundamental precaution for the management to reduce as much as possible the operational risks, which impact on the operations of the business. In the event that part of the activities are outsourced, it is fundamental to guarantee the resilience of such activities. This requires a careful consideration of the activities outsourced by the organization and the characteristics, capacities, and capabilities of the outsourcers. They must be resilient. In other words, they must be able to take into account the potential risks and disasters and be prepared to respond effectively.

In order to cope with the risks of outsourcing, it is essential a defined strategy for resilience. This implies:

- Understand the critical risks connected with outsourcing, and how they are both a technical and a business issue that could impact the continuity of the business of the outsourced customer while wreaking financial havoc;
- Consider how step-change capability improvements can create a more resilient outsourcing environment;
- Discuss how the mentioned nine C's could improve the resilience;
- Explore how the active engagement of business and outsourcer management at all levels can achieve progress toward a better resiliency.

References

'-, About Resilience, *Resilient Organizations*, http://www.resorgs.org.nz/Content/what-is-organisational-resilience.html, Accessed 01 January 2016.

'- (2007), Encyclopædia Britannica 1, London: Encyclopædia Britannica, Inc., London, UK, Accessed 1 January 2016.

'- (2015), Cyber-Resilience in Supply Chains, *Technology Innovation Management Review*, Apr.

Andersen, B., and Fagerhaug, T. (2006). *Root Cause Analysis: Simplified Tools and Techniques*. ASQ Quality Press, Milwaukee, WI.

Bovaird, T. (2016), The ins and outs of outsourcing and insourcing: what have we learnt from the past 30 years?, *Public Money and Management*, 36:1, 67-74.

Carrozzi, L. (2009), *Procurement Management per la Protezione delle Infrastrutture Critiche,* Tesi Master in Procurement Management, Università di Tor Vergata, Rome, Italy.

Carvalho, H., Barroso, A. P., Machado, V. H., Azevedo, S., and Cruz-Machado, V. (2012), Supply chain redesign for resilience using simulation. *Computers & Industrial Engineering*, *62*(1), 329-341.

Christopher, M., and Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International journal of physical distribution & logistics management*, *34*(5), 388-396.

Gonzalez, R., Gasco, J., & Llopis, J. (2005), Information systems outsourcing risks: a study of large provider. *Industrial management & Data systems*, *105*(1), 45-62.

Gulati, R. (2013), *Reorganize for resilience: Putting customers at the center of your business*. Harvard Business Review Press, Boston, MA.

Handfield, R.B. and Nichols, E.L. (1999), *Introduction to Supply Chain Management*, Pearson, Upper Saddle River, NJ

Kaplan, J.M., Bailey, T., O'Halloran, D., Marcus, A., Rezek, C. (2015), Beyond Cybersecurity: Protecting Your Digital Business, Wiley,

Kleindorfer, P.R., and Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and operations management*, *14*(1), 53-68.

Kolodner, J. (2014). *Case-based reasoning*. Morgan Kaufmann, Burlington, MA.

Kunreuther, H. and Heal, G. (2004), Interdependent security: the case of identical agents, *Journal of Risk and Uncertainty*, 23 (2), pp 103–20

Montani, S.and Anglano, C. (2008), Achieving self-healing in service delivery software systems by means of case-based reasoning, *Applied Intelligence*,*28*(2), 139-152.

Nicoletti, B. (2012), *The Methodology of Lean and Digitize*, Gower, London, UK.

Nicoletti, B., (2012), Global sourcing e gestione dei rischi, *Strategie & Procurement*, 10(1), 18-19.

Nicoletti, B., (2012), Rebalancing global sourcing risk, *Procurement Leaders*, May.-Jun., 38.

Osei-Bryson, K. M., and Ngwenyama, O. K. (2006). Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts. *European Journal of Operational Research*,*174*(1), 245-264.

Prieto, B, Plumbee, J. and Vaughn, D (2015), Resilience: An Engineering and Construction Perspective; http://www.lulu.com/shop/robert-prieto/resilience-an-engineering-construction-perspective/paperback/product-22246190.html, , Accessed on 29 Dec. 2015.

Prieto, B, Plumbee, J., Vaughn, D. and Vaughn, J. (2015), Resilience: Managing the Risk of Natural Disaster, *Fluor*, http://www.lulu.com/shop/robert-prieto/resilience-managing-the-risk-of-natural-disasters/paperback/product-22219550.html, Accessed on 29 Dec. 2015.

Pereira, R. C., Christopher, M., and Lago Da Silva, A. (2014). Achieving supply chain resilience: the role of procurement. *Supply Chain Management: An International Journal*, *19*(5/6), 626-642.

Sullivan, W. E., and Ngwenyama, O. K. (2005), How are public sector organizations managing IS outsourcing risks? An analysis of outsourcing guidelines from three jurisdictions. *Journal of Computer Information Systems*,*45*(3), 73-87.

Tierney, K. and Bruneau, M. (2007), Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction, *TR News*, May-Jun., No. 250: 14-16.

Turner, N. and Kutsch, E. (2015), Project Resilience: Moving beyond traditional risk management, *PM World Journal*, 4(11).

Waters, D. (2011), *Supply chain risk management: vulnerability and resilience in logistics*, Kogan Page Publishers, London, UK.

Wüllenweber, K., and Weitzel, T. (2007). An empirical exploration of h240c-240cow process standardization reduces outsourcing risks. *System Sciences*, 2007. IEEE, January, 240-250.

About the Author

Bernardo Nicoletti

Rome, Italy

Bernardo Nicoletti is a lecturer at the Università di Tor Vergata, Rome, Italy. He serves as a Director in Transigma Emea, a strategy consultancy company specialized in process improvements and digitization in financial services with global assignments.

Bernardo has been active in procurement. He applies an innovative approach of Lean and Digitize in his consultancy and has described the methodology in one of his books on Lean and Digitize, published by Gower Press.

Bernardo worked with GE Capital as Program Manager of a Global Payment System, as CTO of GE Capital, and with AIG as CIO Latin America.

Cell: +39 348 470 7016

E-mail: info@bernardonicoletti.com

Web Site: www.bernardonicoletti.com

Blog: www.leandigitize.com