Risk Management Model in ITIL

Sarah Vila-Real Vilarinho

Friday, June 29, 2012

ITIL is considered a framework of best practice guidance for IT Service Management and it is widely used in the business world. In spite of this, ITIL has some gaps in Risk Management specification. There is just a coordination of exercises instead of a clear and owned process, what can limit the efficiency of ITIL implementation in organizations. Our work approaches this problem and compares IT risk management in ITIL to other IT Governance Frameworks. Despite ITIL stating that risk should be identified, measured and mitigated, it is not clear how to proceed (no concrete process is defined on how to deal with risk). To solve this, we propose to map the M_o_R risk management framework in ITIL, mapping every M_o_R process in ITIL, and therefore adopt a strong risk management in ITIL, based on specific guidelines, without changing the framework. Besides this, we propose the introduction of new elements in the risk management ITIL process such as KRIs and a new process responsible for define risk management and guide risk management implementation in the other processes. With this model we present its theoretical application and evaluation by experts. In the end we will show a planning for future work.

1. Introduction

Risk management is a vital part of business nowadays. Some readers think that only innovative businesses need risk management, and that there is no risk in a conservative business. However, this is not true. There is risk in all organizations since its creation until its dissolution. Before delving into the details of risk management, it is important to define what risk is.

1.1. Risk

Risk is defined as uncertainty of outcome; it can be an opportunity or a threat (1). The threat comes from some vulnerability of the organization but, in fact, it is important to take risks for the business evolution. Nevertheless, it is vital to take risks with some precaution and to always define contingency plans for when things go wrong. Every organization manages its risk in some way.

There are several definitions of risk management. According to the authors of “The Essential of Risk Management” (2), it is a process of understanding cost and efficiently managing unexpected levels of variability of the organization. However, each one of the several existing frameworks as well as every existing framework has its own definition, albeit at its core, all of them share the same underlying goals. Managing risks requires the identification, analysis and control of the exposure to risk. The following picture summarizes the risk management process:

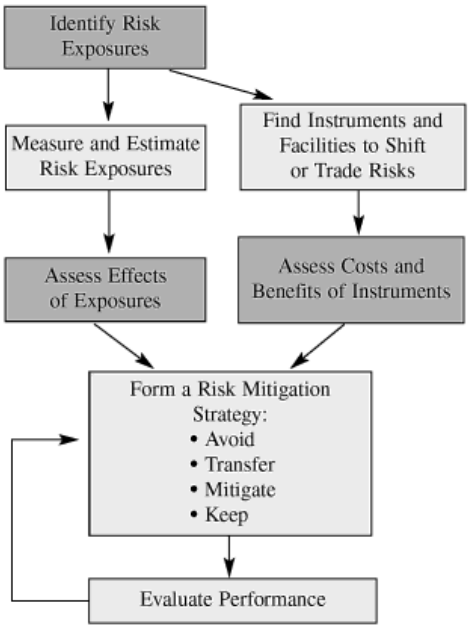

Fig. 1. Risk Management. Source: "The Essential of Risk Management" (2).

The **identification** of risks is the process of identifying threats, vulnerabilities, or events that may have an impact on the set of assets owned by the organization (3). This identification can also be about opportunities (1), but not all risk management frameworks explore this (4). For risk identification, experience is important because it is common for the risk source to derive from a non-deterministic cause.

After identification comes the **analysis** of the identified risk. Risk analysis is concerned with the gathering and measuring of information about risk exposure, so that the organization can make suitable decisions and manage risk appropriately. Finally, risk **control** involves monitoring the environment for improved effectiveness against the previous set of threats, vulnerabilities, or events and make decisions about them. These decisions can be to avoid, mitigate, transfer or keep the risk (2). Once again, the actual process can vary according the framework used.

Every organization has a kind of risk management that is not always explicit, well-structured or consistently applied to support decision making (5). The task aim of risk management is to ensure that the organization makes a cost-effective use of a risk framework that has a set of well-defined steps. The aim is to better support more critical decision making through a good understanding of risks and their likely impact in order to achieve competitive advantage (6).

IT risk management has the same goals and steps of risk management in general.

1.2. ITIL

ITIL is the abbreviation for the guideline IT Infrastructure Library and was developed by CCTA, in Norwich, England, on behalf of the British government (7). The CCTA is currently the Office of Governance Commerce (OGC) (5). As said by the ITIL Foundation in IT Service Management, ITIL is accepted as the Best Practices for lowering process costs while improving the quality of IT services delivered to users. It is derived from the practices of the most successful and effective people in the field (8). Therefore, it would be useful to explore risk management in the context of this framework.

2. Research Problem

Nowadays all organizations have a very strong relationship with IT, most of them are completely dependent on it and it would not be possible to maintain large scale business without IT. To achieve the best return of investment, avoid instability

and add value to an organization, a good risk management is essential. (1)(2). So the risk management on IT Service Management is an indispensable component.

We have uncountable guidelines, frameworks and tools designed to support risk management and IT Service Management. To implement an IT Service Management framework, ITIL is usually the option. However, the information about risk management in the ITIL Library is generalist and unsatisfactory. Compared with other IT service management frameworks, ITIL is weak in the risk management field (3). This forces organizations to the implementation of a risk management framework parallel to IT Service Management which leads to a loss of efficiency and detail.

ITIL V3 has as a base for risk management the concept of "coordinated risk assessment exercises" (3) (4), a coordinated set of activities to identify and assess vulnerabilities and control risks. The major problem of these exercises is that they do not assign clear responsibilities for managing risks and it they are not sufficient to manage all IT services in an ITIL context. There are no triggers to start these "exercises", there are no formally defined inputs or output, there are risk management elements missing and a transversal approach is not clearly defined. Of course every book has a section on "risks", but those sections are a definition of what is risk and not exactly a explanation about how to proceed to cover risk management.

In short, despite risk management being referenced in ITIL books, **this approach is not explained enough for the organizations to implement risk management without following specialized guidelines for it**. So, for an organization, the big issue is to adopt a strong risk management in ITIL (and turn ITIL more competitive in this field in comparison with other IT service management frameworks that have much more defined guidelines on this subject, like COBIT) in an integrated, effective and efficient way, without changing the framework, so that organizations do not have to use another mechanism for risk management.

3. Related work

There are several framework proposals for risk management (5) and ITIL implementation. However, so far there is not a satisfactory integration between these standards (6), and the fact is that ITIL does not cover Risk Management properly. Organizations are still looking for the best set of practices to apply to business. Some researchers have concluded that the key for a successful strategy is a combination of various methodologies and tools (5) (6) (7).

According nowadays publications risk management has not been able to prevent, in a consistent way, market disruptions or to prevent business accounting scandals resulting from breakdowns in corporate governance (8) and specially in ITIL(3).

Risk management has some well-known gaps but sometimes its progress depends on the failure of previous experiences. Nevertheless, sometimes these failures occur only because risk management is not well implemented (9). This happens because often managers do not know how to do it efficiently.

In ITIL there are some clues about how to implement risk management across the framework, about the tools and the risks that are already known. However, the information in the ITIL Library is still unsatisfactory.

Despite M_o_R being referred to in ITIL Books, it is unclear if this is the official way to treat risk and how to implement this risk management framework in ITIL. The tool list for risk assessment is not complete and the information is too vague.

Some risks are enumerated in the Service Operation book but there are no guidelines on how to deal with them.

In Daniel Deusing's article (9), there is a guideline about how to implement risk management in ITIL that seems to be very useful.

Process	OGC	Critical Analysis
Problem Management	There is a proactive and reactive management, with the goal of reducing the impact of service outages.	They do not specify how the actions that need to be done (e. g. disaster covered plan) are predicted and implemented.
Change Management	Good change management techniques and approach help reducing risks, minimize the potential negative impact of change, and reduce the risk of an undesirable outcome.	What techniques and approaches should be implemented? (10) A specific one is not mentioned.
Service Delivery	Services must be maintained, so it is important to have a careful design.	Besides the careful design, how to maintain service delivery must be specified as well as plans to recover from threats.
Availability Management	Focuses on reliability and on how to put in place alternative options to ensure the service continues.	
IT service Continuity	Assesses risk to ensure overall continuity for the business.	They do not specify how to implement risk management across all modules.

Table. 1. Risk management coverage according to OGC and critical analysis.

In Wickboldt's article (10), a representation model is proposed in order to obtain feedback from the execution of changes over an IT Infrastructure in which the process of record changes should be automated.

On the one hand, risk analysis would allow human operation to be more precise and quick and so to react more efficiently. On the other hand, the change management process is just a part of the risk management gap in ITIL and it is not possible to automate all the process.

4. Model Proposal

This model has at its foundation the related work, the experience of experts in the field and our own experience with an ITIL oriented tool (Easyvista) and Methodology. Its main elements are:

- The new **Risk Management process (broken into two parts)**;
- The definition of **KRI** amid ITIL;
- **Mapping of M_o_R processes** in ITIL sub-processes;
- **Reinforcing of ITIL risk management concepts** such as CSF, a potential risk and strategic response to all ITIL processes.

To sum up this model combines a set of concepts from ITIL, from M_o_R and concepts shared by these two frameworks. The ITIL processes will be reinforced with risk management elements and injected with the new M_o_R concepts referred to in the figure above. Besides the introduction of these new elements, all ITIL processes will be wrapped in M_o_R principles and approaches as is proposed in the M_o_R framework for organization services.

Another main new element is the new risk management process. The goal of the risk management process is to identify, assess and transversally control risks in the organization. But apart from other processes, this one is broken into two.

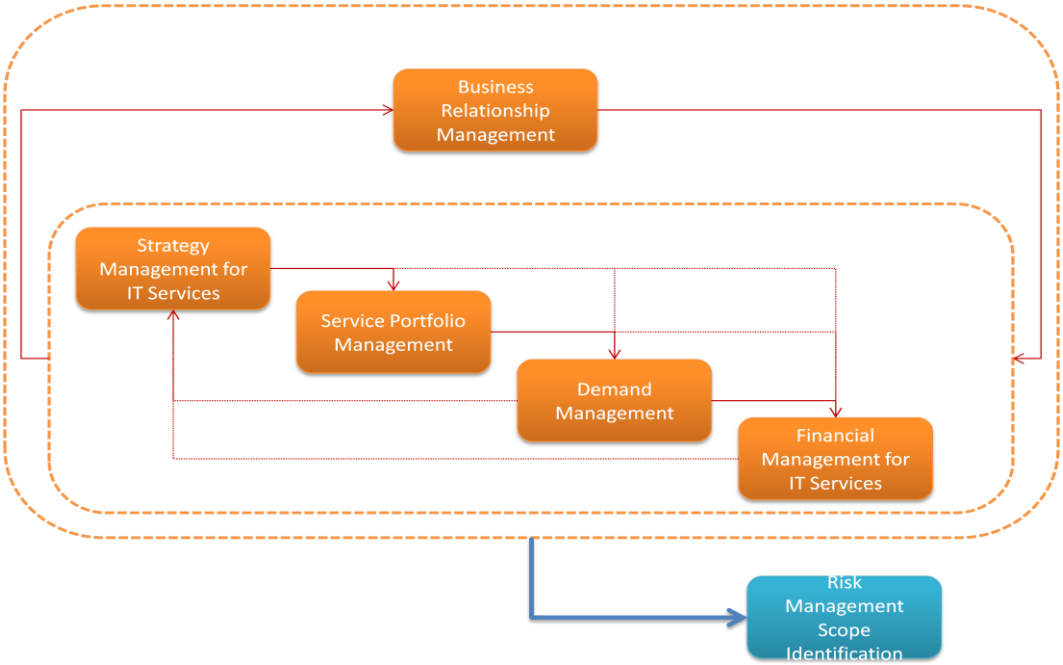

Fig. 2. First part of Risk Management process on Service Strategy

The first part is in Service Strategy and it is responsible for identifying what risks an organization is willing to support. Here is aboard the accountability risk. In this phase an organization will decide on what it can handle and what it cannot based on other Service Strategy outputs. The result is the input used to design the risk management phase.

In the second part, the process focuses on operational risks. The risk management process receives output from Service Strategy and input from other design processes. This includes the analysis of the assets' value to the business, the identification of the threats to those assets, and an evaluation of how vulnerable each asset is to those threats.

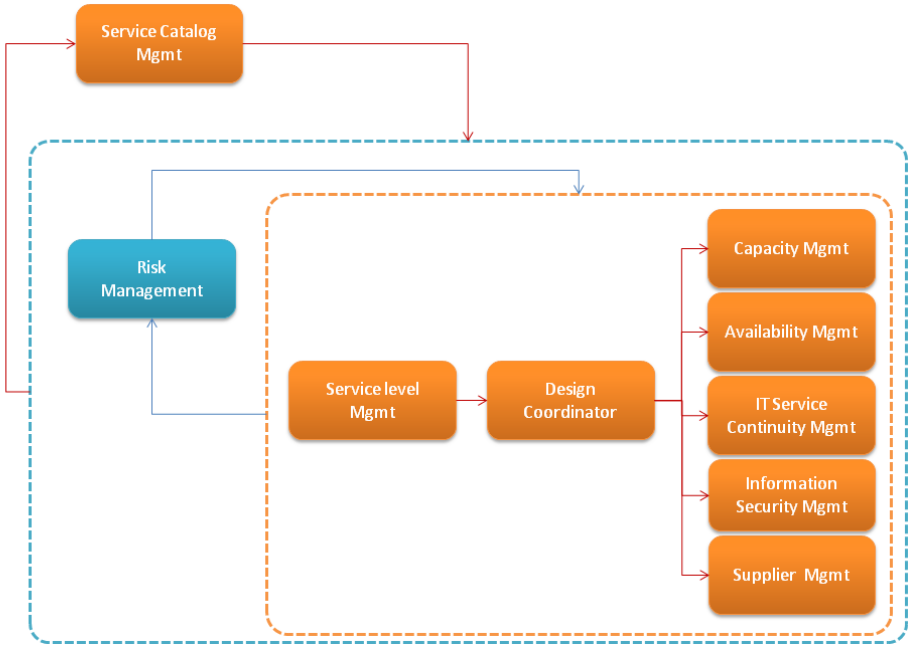

Fig. 3. Second part of Risk Management process on Service Design.

The advantage of including this process in ITIL is having risk management clearly assigned to defined roles, establishing the scope of an organization on Service Strategy and defining the owner process, technique, task as well as inputs and outputs on Service Design, giving risk management a main role in ITIL process and a specialized and continual intervention. In addition, once the output about risk management is formalized, it guarantees predict services with more quality. The formalization of a risk management process is proposed in other ITSM frameworks and is supported by several specialists (3). The design risk management process is responsible for identifying KRIs and CSF with the manager owner of the other processes. The output of this process is a central risk management orientated to each design process that diffused all ITIL processes.

For the existing processes we identified new risk elements: Key Risk Indicators (KRIs), Critical Success Factors (CSF) and the respective strategic response for all potential risks. All ITIL processes must have Risk Management elements according their purpose. Naturally some processes have stronger risk management elements than others, mainly processes that provide input to others (providing a base for other processes).

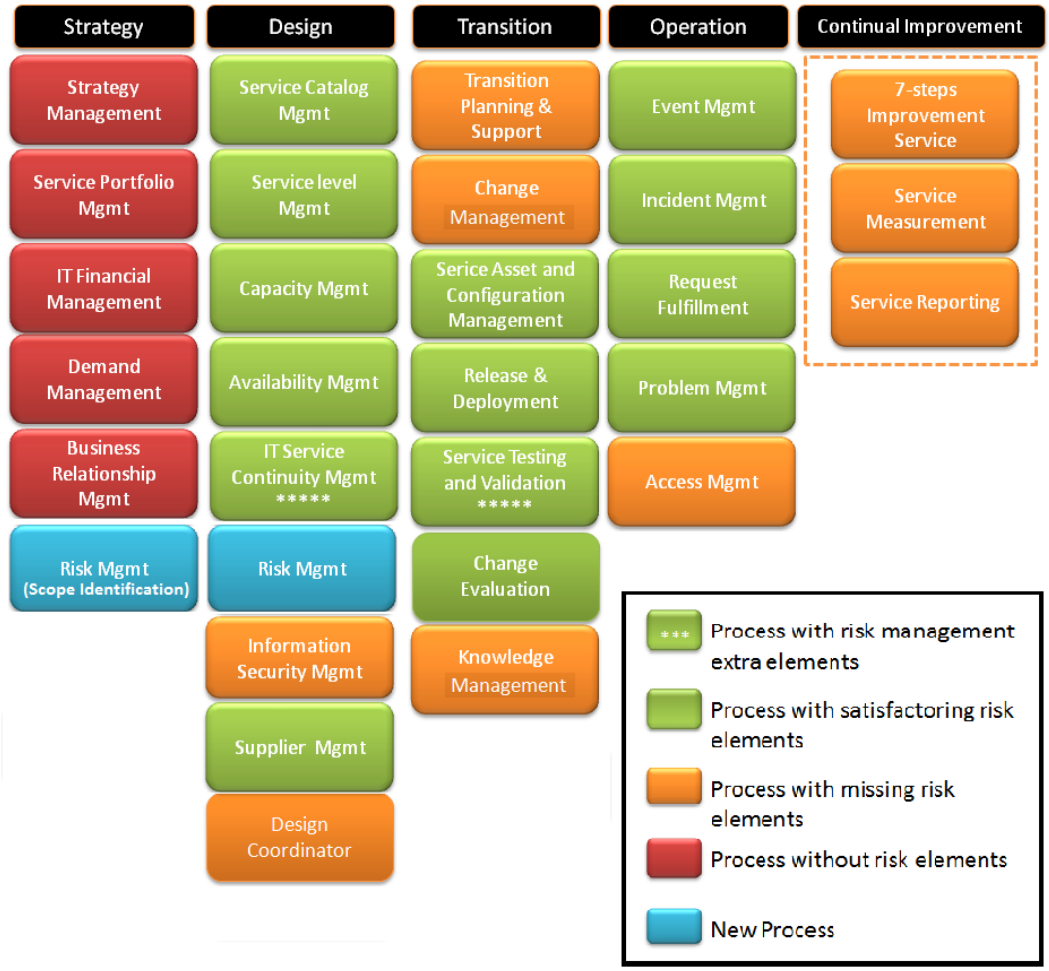

Fig. 4. ITIL process map according risk elements plus new process suggest by our model.

In **Fig. 4** we can notice that, nowadays, in Service Strategy no process clarifies how risk management is embedded. There is no definition of CSF and the potential response is not clear. In the processes in orange we notice a presence of risk management elements but CSF and Risk management elements are not clear. In the processes marked in green, the CSF and a strategic response are defined (but occasionally with some gaps); usually in these processes the CSF and risk management have a defined role on the process. KRIs are not contemplated by ITIL. In the model, the idea is to homogenize the

presence of these risk management elements adding them to the process in which they are not defined. Of course the definition of KRI's in each process must be supported by the risk management process (design phase).

The definition of KRIs is important in the way that it provides a set of risk management guidelines (indicators as the name suggests), making risk management clearer and more efficient. They must be measurable and clear about what they measure.

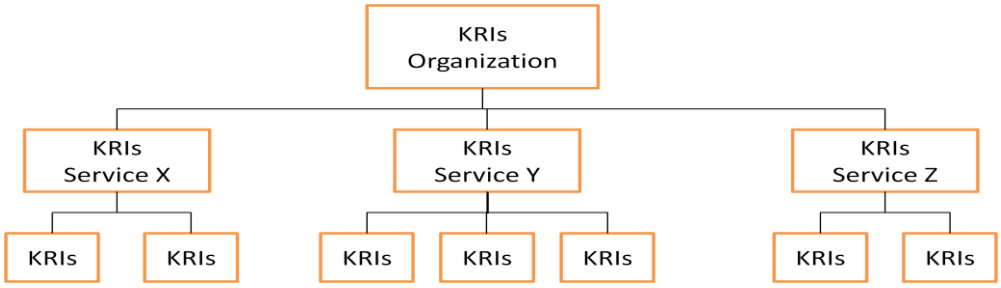

Fig. 5. Work breakdown structure of KRIs

This KRIs must be defined from top to bottom according to the organization structure. It is logical that a large company risk management has several layers. These KRIs must be followed by cost associated to the potential risks and must be estimated for qualified staff.

This document is not inclusive of all KRIs but simply an example of how KRIs may be mapped to processes. The number of KRIs here will be one or two per CSF (Critical Success Factors) as a service or process has no more than two to three associated CSFs. This may not sound much but when considering the number of services and processes, it is a lot. In the organization it is important to define not all KRIs but the ones connected to potential risks that may have a more significant impact in the organization. For all potential risks identified, we defined one or more KRIs and a specific strategic response. However, according to the organization's particularities, this list can be enforced and adjusted, always keeping M_o_R principles in mind.

In this model it is considered that all ITIL Processes have a cycle of M_o_R process (Identify, Assess, Plan and Implementation) that guarantees that M_o_R processes are fully embedded in the ITIL framework. Each M_o_R step is mapped in, at least one, ITIL sub-process. In the figure below, we present an example of one of the strategic services processes mapped with M_o_R Process.

The M_o_R concepts (KRI's, strategic response, potential risks) are mapped inside ITIL processes. But for all this to work it is important to wrap all ITIL processes (at the sub-process level) by M_o_R principles and approach. In accordance to M_o_R, there are 8).

These principles are concerned with achieving outcomes by defending or changing organizational performance. They are used to elaborate strategy and to provide continual improvement. These principles must be applied in a transversal way in all ITIL Process.

Wrapping all ITIL processes, the M_o_R concepts of embedding and review must be integrated in CSI. The details of this integration must be presented and communicated to stakeholders throughout all processes. The pillars are:

- Embedding the principles;
- Changing the culture for risk management;
- Measuring the value;
- Overcoming the common barriers to success;
- Identifying and establishing opportunities for change.

Next we exemplify the application of our model in one ITIL process:

Example (Service Portfolio Management):

Service Portfolio Management manages the service portfolio. Service Portfolio Management ensures that the service provider has the right mix of services to meet required business outcomes at an appropriate level of investment. The risk management steps assigned to its sub process are:

- **Identify**, **Assess** and **Plan** on Defining and Analyze new or changed Services;
- **Assess** and **Plan** on Approve new or changed Services;
- **Implement** on Service Portfolio Review.

And the critical success factors are:

- Create planned and Unplanned services that fits in customer necessities;
- Determine The capability of services and adjust it according customers amount;
- Keep the Service Portfolio up to date.

Having the process goals in mind, the main risk management elements are:

Potential Risk	KRI (Key Risk Indicators)	Strategic Response
Creation of a service that is not align with organization strategy or organization/customer.	Decrease/Increase of customers satisfaction. Decrease /Increase of customer.	Analyse the impacts on existing and the creation of new services in the organization and determine the assets required to offer the service.
Customer number variation.	Decrease /Increase of customer. Rate of service utilization.	Determine the amount max and min of customers for provide a service (costs, profits). Elaborate a plan in case of variation of customers. Controlling the amount of customers through lists, reports and properly documentation (according to M_o_R recommendations).
Not keeping the Service Portfolio up to date.	Number of services registered in the services portfolio.	After approved the service must be formally identified in the Service portifolio and communicated to organization. Creation of Service Portfolio Review Report, A document containing the results and findings from a Service Portfolio Review.

Table. 2. Potential risks, KRIs and Strategic Response for Service Portfolio Management.

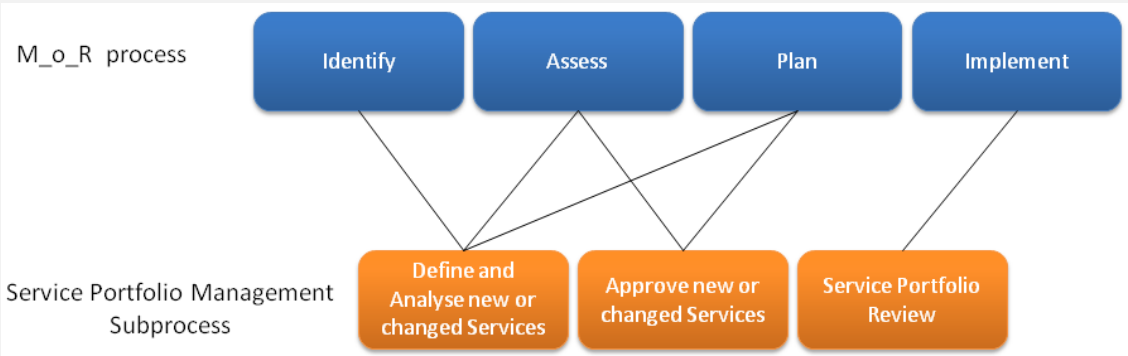

Fig. 6. Example of the M_o_R process mapped on a ITIL sub process.

5. Evaluation

Our evaluation process has at its core the evaluation of our proposed model with a set of experts in the field of ITIL and IT risk management.

The experts' opinion was gathered using three different methods:

- The publication of a research article at the Centeris conference, outlining our research problem and the scope for our proposed model;
- The ITIL group discussion on LinkedIn and Facebook social networks;
- Direct approach to experts in Portugal and Brazil.

ITIL experts were chosen according to three criteria:

- To be able to articulate their opinion about the model;
- Depending on their certification and work experience;
- Their availability.

The experts' opinion shows that the several project managers identify risk management in ITIL differently. Some of them identify risk management as belonging to the Design module while others say that risk management should be embedded on CSI. This is not wrong. However, what is intended with this model is to clarify risk management artifacts.

There is no consensus about the need of a risk management process in ITL. It is not clear to all of experts, maybe because each manager sees risk management in ITIL in their own way. Actually, in the organizations nowadays, risk management is a completely separate process that includes not only IT, but all the organizations

6. Conclusion

The risk management is essential to all organizations. There are several framework proposals for risk management but for organizations where ITSM is a big part of business it is important to simplify the process. So it is desired to congregate business modules such as risk management and ITSM.

The value of ITIL is undeniable these days as reducing IT costs, increasing IT performance and, at the same time, improving business performance through IT-business alignment. These qualities are vital for any organization.

We think that for this would be important:

- Integrate/adapt a risk management framework to embed in ITIL;
- Document methodologies to deal with risk in ITIL process;
- Create elements to measure risk exposure and link them to strategic responses.

What we tried to do here was to clarify the risk management embedding on this framework and reinforce it. For this we clarified and adjust the place of M_o_R on this framework, mapping M_o_R process on ITIL sub processes and add two important points:

- KRIs;
- A new process response for risk management on Design Module.

This difference helps the organizations board and stakeholders to deal with risk, giving them a guideline about how risk management must work on an organization and giving metrics to identify the risk management elements and the proper strategic response.

7. References

1. **Crouhy, Michel, Galai, Dan and Mark.** *The Essentials of Risk Management.* s.l. : McGraw-Hill, 2005.

2. *A Importância do Gerenciamento de Riscos Corporativos.* **Júnior, Antonio M. D.** Brazil : s.n., 2010.

3. *IT Process Map.* [Online] http://wiki.en.it-processmaps.com.

4. *ITIL V3 and Information Security.* **Clinch, Jim.** London : OGC, 2009.

5. **Raz, Tzvi and Hilson.** A Comparative Review of Risk Management Standards. *Risk Management: An International Journal.* 2005, pp. 53-66.

6. **Raz, Nicolas, Weippl, Edgar and Seufert.** A process model for integrated IT governance, risk, and compliance management. *Databases and Information Systems. Proceedings of the Ninth International Baltic Conference.* 2010, pp. 155-170.

7. **Cater-Steel, Aileen, Tan, Wui-Gee and Toleman.** Challenge of adopting multiple process improvement frameworks. *Proceedings of 14th European Conference on Information Systems (ECIS 2006).* Goteborg, Sweden : USQ, epEditor, 2006, pp. 1375-1386.

8. **Office of Government Commerce.** *ITIL - Service Design.* London : OGC, 2007.

9. **Deusing, Daniel.** *ITIL and Risk Management.* Hochschule Furtwangen University : s.n., 2010.

10. **Wickboldt, Juliano Araújo, et al.** A Solution to Support Risk Analysis on IT Change Management. Piscataway, NJ, USA : IEEE Pres, 2009, pp. 445- 452.