INSTITUTO SUPERIOR TÉCNICO
Universidade Técnica de Lisboa

Risk Management Model In ITIL

Sarah Vila-Real Vilarinho

Dissertation for the Degree of Master of

Information Systems and Computer Engineering

Jury

President:	Prof. Dr. Joaquim Armando Pires Jorge
Supervisor:	Prof. Dr, Miguel Leitão Bignolas Mira da Silva
	Prof. Dr. Maria do Rosário Gomes Osório Bernardo Ponces de Carvalho
Member:	Prof. Dr André Ferreira Ferrão Couto e Vasconcelos

June 2012

Acknowledgment

In the first place I would like to thank to Instituto Superior Técnico for the opportunity to produce this thesis and to enlarge my scientific background. In particular, I would like to thank professors Miguel Mira da Silva and Maria do Rosário Carvalho, whose patience, help, advice and supervision were invaluable.

I would like to thank all the experts who dispended their time evaluating and inspiring some parts of my work.

I would also like to thank to my friends, my uncles (Cláudia and Marcos) and all my work colleagues for their support and understanding, especially to my friend Pedro Jacinto for his huge support, reviewing and criticizing during my work. Without his support probably I would not finish this thesis.

Abstract

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. In fact, there is only a coordination of exercises instead of a clear and owned process, which can limit the efficiency of ITIL's implementation in organizations. The present thesis approaches this problem and compares IT risk management in ITIL to other IT Governance and service management frameworks. Despite ITIL stating that risk should be identified, measured and mitigated, it is not clear on how to proceed (since no actual 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, and adopting a strong risk management, which is 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 defining risk management that can help guide risk in other processes. With this model we present its theoretical application in Disney's ITIL implementation and some experts' evaluation of the model. Finally, we suggest a proposal for future work.

Keywords: Risk Management, ITIL, M_o_R, KRI, risk

Resumo

ITIL é considerado a framework de melhores práticas em gestão de serviços IT e é amplamente usado no mundo dos negócios. Apesar disso, o ITIL tem algumas lacunas na definição da gestão do riscos.Em vez de um processo claro e com responsabilidades claras, há apenas um conjunto de exercícios coordenados, o que pode limitar a eficiência da implementação ITIL nas organizações. Esta tese aborda este problema e compara o gerenciamento de risco em ITIL com outras frameworks de governance e gestão de serviços de TI. Apesar doo ITIL afirmar que os riscos devem ser identificados, medidos e mitigados, não está claro como proceder (nenhum processo concreto é definido sobre como lidar com o risco). Para resolver isso, nós propomos o mapeamento da estrutura de gerenciamento de risco M_o_R no ITIL, mapeando todos os processos M_o_R em ITIL e, portanto, adotando uma gestão de risco robusta, baseada em diretrizes específicas, sem alterar a framework. Além disso, propomos a introdução de novos elementos no processo de gestão de risco, tais como KRIs e ainda um novo processo responsável por definir gestão de risco e que tem como objetivo guiar a gestão do risco nos outros processos. Com este modelo apresentamos também uma aplicação teórica a implementação do ITIL na Disney e avaliação do modelo por peritos. No final, mostraremos sugestões e planeamento para o trabalho futuro em cima do modelo.

Palavras chave: Gestão do Risco, ITIL, M_o_R, KRI, risco

Table of Contents

List of Figures

List of Tables

Abbreviations

AMIS - Availability data into an integrated set of information
BCM - Business Continuity Management
CAPA - Corrective and Preventive Action
CCM - Component Capacity Management
CCTA - Central Computer and Telecommunications Agency
CMS - Configuration Management System
CSF - Critical Success Factor
CSI - Continual Service Improvement
FMITS - Financial Management for IT Services
IS - Information Systems
IT - Information Technology
ITIL - Information Technology Infrastructure Library
ITSCM - ITIL Service Continuity addresses Risk
KPI - Key Performance Indicator
KRI - Key Risk Indicator
OGC - Office of Government Commerce
OLA - Operation level agreements
QoS - Quality of Service
RDM - Release and Deployment Management
RMC - Rational Method Composer
ROI - Return on Investment
SACM - Service Asset and Configuration Management
SCM - Software Configuration Management
SCMIS - Supplier and Contract Management Information System
SKMS - Service Knowledge Management System
SMITS - Strategy Management for IT Services
SLM - Service Level Management
TWDC – The Walt Disney Company
UC - Underpinning Contract

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 Management

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:

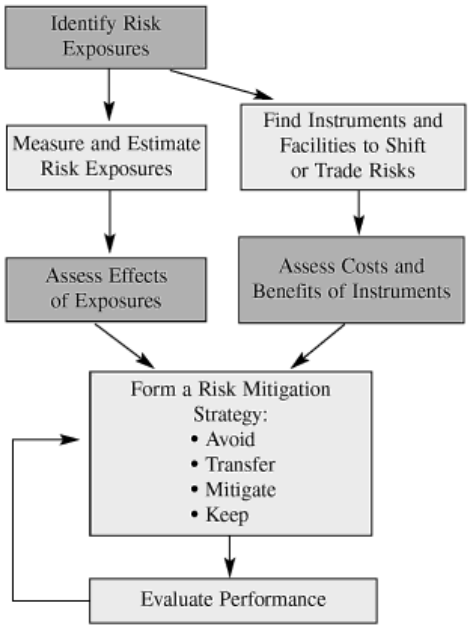

Fig. 1. Risk Management. Source: (2).

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 Framework

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.

1.3. Research Problem

The research problem approached in this document focuses on risk management in multi-unit organizations (organizations that do not focus exclusively on IT). However, the scope is focused on risk management in IT.

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. (2)(9). 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 (10). This forces organizations to implement a risk management framework that runs in parallel with IT Service Management, which leads to a loss of efficiency and detail.

The following figure outlines the main components of the scope of the research problem.

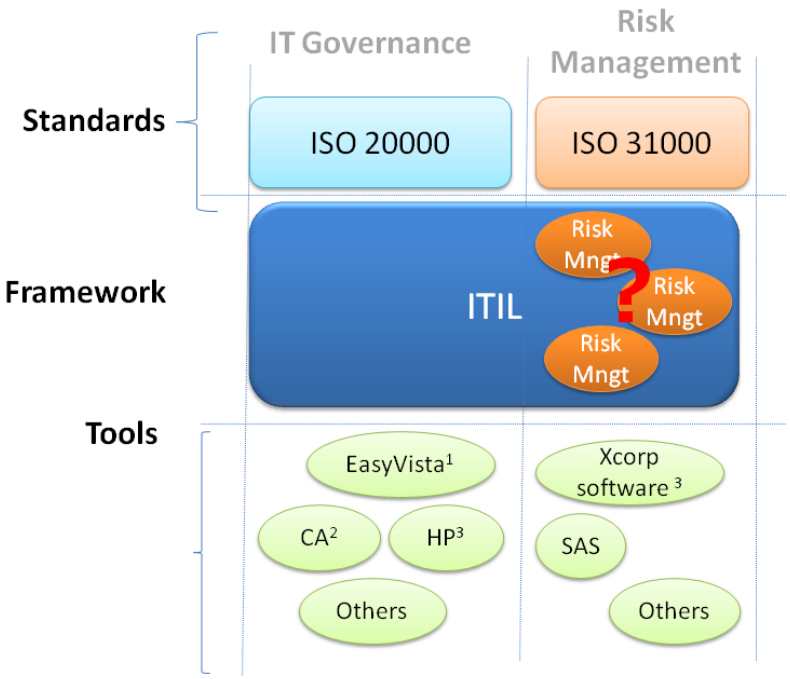

Fig. 2. Problem context.

ITIL V3 has the “coordinated risk assessment exercises” (10) (11) concept as a base for risk management, which includes a coordinated set of activities that 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 they are not sufficient to manage all IT services in an ITIL context. There are no triggers to start these “exercises” and no formally defined inputs or outputs. In addition, there are risk management elements missing and a transversal approach is not clearly defined. Of course every book has a section on "risks", but these sections are a definition of what risk is and not exactly an explanation on how to proceed to cover risk management.

In short, despite risk management being referred to in ITIL books, **this approach is not explained enough for 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 make 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.

1.4. Research Methodology

The definition of the research methodology is extremely important. It is more than a set of skills, it is a way of thinking. It indicates how the search of knowledge and the investigation will be made. The research methodology used in this work will be the Design Research (12).

The design-science appeared around the sixties and has its roots in engineering and the sciences of the artificial. This methodology involves the analysis of the use and performance of design artifacts in order to understand, explain and improve the behavioral aspects of Information Systems (12).

The Design Research Method is best suited for scenarios involving (13):

- Unstable requirements and constraints based upon ill-defined environmental contexts;
- Complex interactions among subcomponents of the problem and its solution;
- Inherent flexibility to change design processes as well as design artifacts (i.e., malleable processes and artifacts);
- A critical dependence upon human cognitive abilities (e.g., creativity) to produce effective solutions;
- A critical dependence upon human social abilities (e.g., teamwork) to produce effective solutions.

After comparing the characteristics of design problems and our problem, which is a complex interaction between risk and ITIL and which depends on the managers' experience and ability, it is clear that this research method is the best choice.

Comparing the Design Research phases and thesis expected contributions the result is the next table:

Phase	Outputs
Identify Problem and Motivate	State of art - Preliminar thesis report
Define Objectives of a Solution	
Design and Development	The Artifact - Clarify and introduce Risk management elements in ITIL (see section 3 - Model Proposal)
Demonstration	Disney's case (section 4 - Demonstration)
Evaluation	Experts' opinion (see section 5 - Evaluation)
Communication	The Dissertation - This Document

Table. 1. Thesis' Contribution

The phases of Design Research in our work consist of (14):

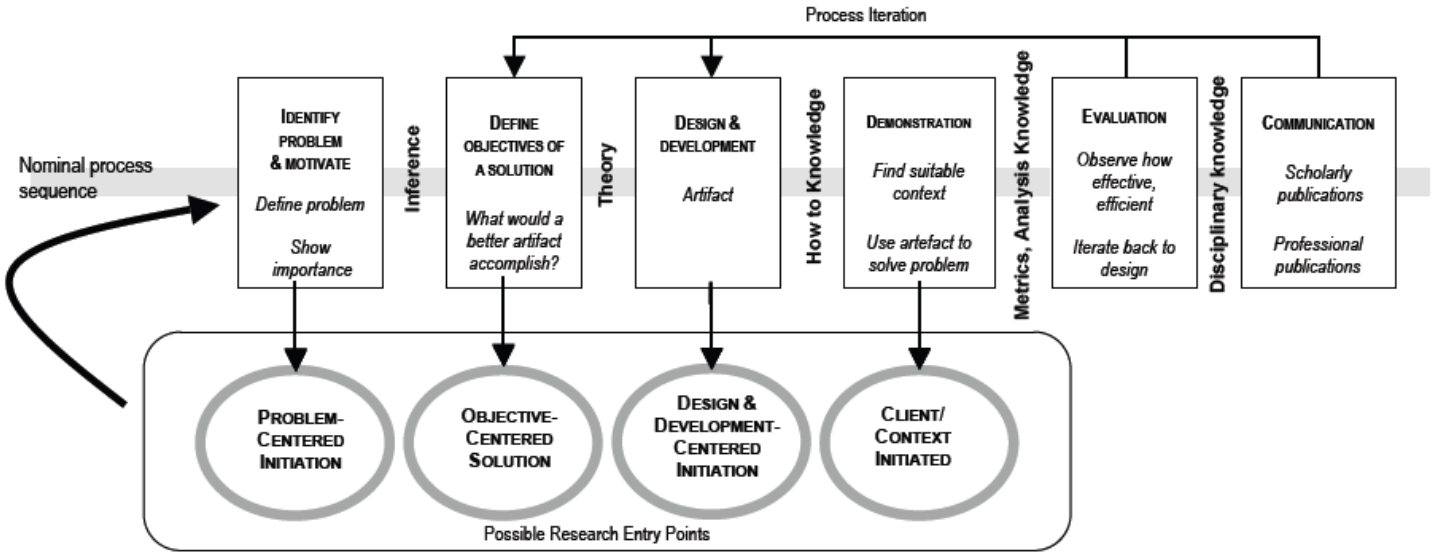

Fig. 3. Design Research Cycle. Source: (14).

- **Identify Problem and Motivate:** Define the specific research problem - the absence of robust risk management guidelines in ITIL - and justify the value of a solution. It happens as a result of a study of the ITIL framework and the current IT and risk management best practices. The resulting output is the purpose.
- **Define Objectives of a Solution:** Intimately connected with the Identify Problem and Motivation stage, this is the phase that ensures the creation of something new in the process of creation of this model. The goals of the solution are inferred from the problem definition and knowledge of what is possible and feasible. In this phase, the output is our model.
- **Design and Development**: In this phase our model will be designed and implemented through the systematic identification of KRIs in ITIL processes. The techniques used will be the combination of elements from different frameworks (ITIL and a risk management framework) in order to construct a robust model to deal with risk management in ITIL. For this we rely on the ITILand M_o_R recommendations as well as the opinion of experts. We will also use our own experience from real organization's projects to build this model.
- **Demonstration:** The Disney case is a demonstration of the model propose and it will consist in a theoretical implementation of our model in order to exemplify the application of the model in concrete scenario. It allows us to make a more formal evaluation of our model and to clarify its implementation.
- **Evaluation:** In this phase, the model will be observed by experts in the field and it will be evaluated as a possible solution to the problem. These criteria will be explained in the evaluation section in detail. The evaluation can confirm or contradict the initial hypothesis. Until a satisfactory conclusion is reached, we can reformulate the hypothesis and start a new cycle. When an acceptable conclusion will be reached, the research process can move forward to the communication step.
- **Communication** (Conclusion): Communicate the problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences. This communication will be done through this document.

1.5. Document Structure

This document is structured as follows:

- **Section** 1 **- Introduction**: A short introduction about the general context in which our study is placed, risk management, ITIL, our research problem and its underlying motivation, the study's goals and the research methodology used.
- **Section** 2 **- Related Work**: Our Theoretical Background and related work, introducing the solution structure.
- **Section** 3 **- Model Proposal**: In this section we outline our proposed model to simplify and clarify the implementation of risk management in organizations, proposing some new elements of risk management inside the ITIL process and making risk management possible without using an extra framework
- **Section** 4 **- Demonstration**: A theoretical implementation in a real case study.
- **Section** 5 **- Evaluation**: this section presents experts' opinion and their analysis concerning the model.
- **Section** 6 **- Conclusion**: A short conclusion about this study, reflection and proposals for future work.

2. Related Work

There are several framework proposals for risk management (4) and ITIL implementation. However, so far there is not a satisfactory integration between these standards (15), 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 (4) (15) (16). In this section we will consider what has been written about Risk management, its frameworks, standards and tools, ITIL, ISO 20000 and the combination of risk management and governance, with a special focus on ITIL.

2.1. IT Risk

Although risk management is a subject that is widely discussed nowadays, it is still often approached in an amateur way. It is common for it to be done with very archaic tools, without any integration with governance and sometimes without a shaped plan.

According to the European Network and Information Security Agency (ENISA) the major problems in risk management include (3):

- Low awareness of risk management activities within the public and private sector organizations;
- Absence of a “common language” in the area of risk management to facilitate communication among stakeholders;
- Lack of surveys on existing methods, tools and good practices;
- Limited or nonexistent interoperability of methods and integration with corporate governance.

Another issue is the use of tools to support risk management. In the *Use and benefits of tools for project risk management* article (17), a large number of tools to support the various phases of the risk management process are shown and those associated with successful projects are highlighted. Although this is an old study, we can realize that the best tools are associated with documentation and quality methods(17).

Another element used to support risk management are the metrics. These metrics help the management and the board to be in a better position to manage future events. There are two metrics that stand out: the Key Risk Indicators (KRI) and the Key Performance Indicators (KPI).

While KPIs provide a high-level overview of the performance of the organization, they focus exclusively on its historical performance and key units and operations, while KRIs provide timely leading-indicator information about emerging risks. In some cases, KRIs may represent key ratios that the management (throughout the organization) tracks as indicators of evolving risks, and potential opportunities, which point out the need for actions to be taken. Others may be more elaborate and involve the aggregation of several individual risk indicators into a multi-dimensional score about emerging events that may lead to new risks or opportunities (18).

In Tzvi, Raz and David Hillson’s study (17), the authors compare some risk management frameworks and conclude that they have the same understanding of what risk management should

cover, and similar structure of the process despite having a different scope (some focus on the project and some focus on the organization). However, the main differences among them are concerned with:

- The inclusion of additional elements beyond the central risk management process such as communication elements, collaboration elements and guides;
- The approach to process - certain standards cover mainly the risk management process itself, and ignore the aspects involved in establishing the organizational infrastructure needed to apply the process;
- The differing definitions of risk among the selected standards, which can be seen in two areas: opportunities or threats. Some frameworks just focused in the risk management of the threats.

Besides the choice of a framework, its implementation is still an issue. Luis Nascimento's dissertation (1) is a good study that gathers the current limitations of the implementation of risk management in organizations. In his work it is mentioned the purpose of ISO31000 and the issues concerned with implementing the best practices in real context.

2.1.1. ISO31000

The ISO31000 appeared to provide a consistent approach to risk management. It provides generic guidelines for the principles involved in effective implementation of risk management.

Principles (3) that risk management should have:

- Create Value;
- Be an integral part of organizational processes, should not be a standalone activity, or be separate from the main activities and processes of the organization;
- Be part of decision-making, helping prioritize actions and distinguish among alternative ways;
- Address uncertainty;
- Be systematic and structured;
- Be based on the best available information. Sources should be experience, feedback, observation, forecast and experts' judgment;
- Risk management should be aligned with the organization's external and internal context and risk profile;
- It should take into account human factors;
- Be timely involved and include stakeholders and, particularly, decision makers of all levels of an organization should ensure that risk management remains relevant and up to date;
- Be dynamic, iterative and responsive to change;
- Be capable of continual improvement and enhancement.

There is a framework based on ISO31000 to integrate risk management within its overall management system. The picture bellow depicts the framework described in the Kouns' book (3).

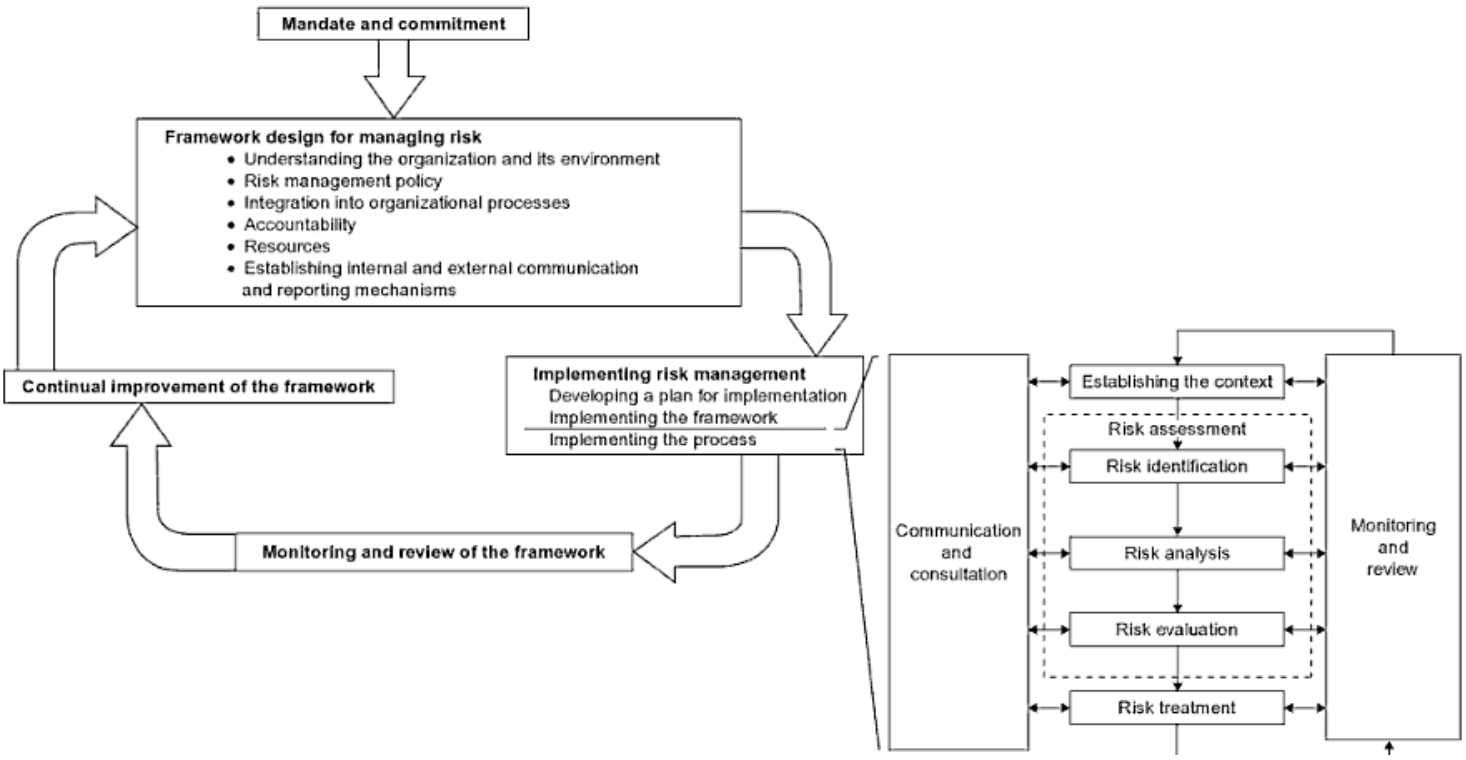

Fig. 4. Framework for Managing Risk per ISO31000 source: (3).

According to this framework, the risk management analysis must be performed following these steps:

Framework design for managing risk

Step 1: Understanding the organization and its environment;

Step 2: Define the risk management policy;

Step 3: Achieve integration in the organizational process;

Step 4: Define Accountability;

Step 5: Identify Resources;

Step 6: Establishing internal communication and reporting mechanisms;

Step 7: Establishing external communication and reporting mechanisms.

Implementing risk management

Step 8: Developing a plan for implementation;

Step 9: Implementing the framework for managing risk;

Step 10: Implementing the process itself;

Step 10.1: Communication and Consultation;

Step 10.2: Establishing the context;

Step 10.3: Developing risk criteria;

Step 10.4: Risk Assessment;

Step 10.5: Preparing and implementing;

Step 10.6: Recording the risk management process;

Step 10.7: Monitoring and review;

Step 11: Monitoring and review of the framework;

Step 12: Continual improvement of the framework.

Although this is a useful and complete set of guidelines about what is expected from a risk management framework in an organization, according to ISO31000, there are some gaps. One of them is the fact that opportunity is not referred to, like in M_o_R.

2.2. M_o_R

The M_o_R is a Risk Management Framework proposed by OGC (19) for risk management and is based on four concepts (6):

- **Principle**: essential to the development of good risk management; it is derived from corporate governance principles, which are based on corporate governance principles and ISO31000 guidelines;
- **Approach**: adaptation of the principles to suit the organization;
- **Process:** describes the inputs, outputs and activities involved in ensuring that risk is identified, assessed and controlled;
- **Embedding and Reviewing:** ensure that principles, approach and process are consistently applied across the organization and that their application undergoes continual improvement in order for them to be effective.

M_o_R considers principles, approach and processes throughout the organization (20). This Framework is linked to other OGC Best Practices in terms of the roles, responsibilities and terminologies used outside the subject of project management. The main diference among the other risk frameworks is the fact that M_o_R emphasizes risks as being either **threats** (downside risks) or **opportunities** (upside risks). Following we depicture the M_o_R cycle.

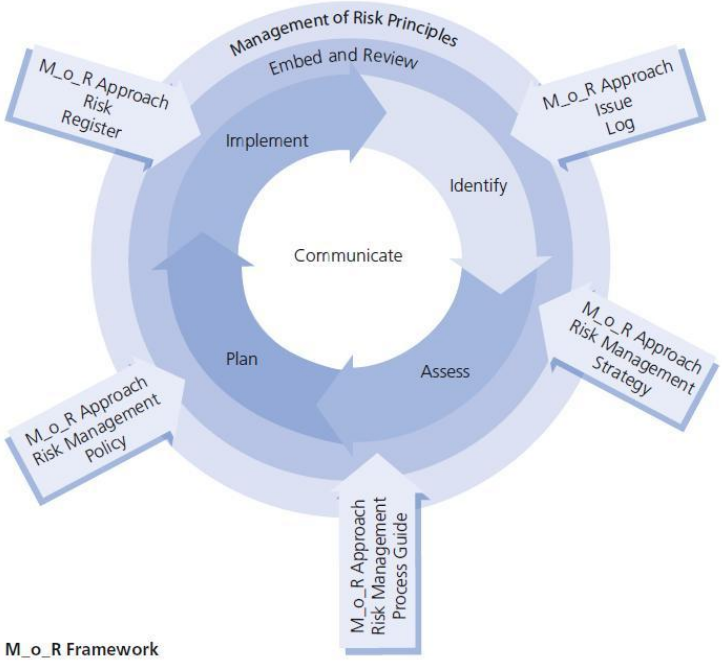

Fig. 5. M_o_R Framework. Source: M_o_R Official Site (19).

We can notice that M_o_R cycle is very similar to ITIL cycle.

2.3. Risk Management Conceptual Map

All Risk Management frameworks share the same basic concepts, tasks and methods and relationships; the main difference among them is the way in which all the elements are combined together. Based on the actual literature we can create a risk management conceptual map, covering the main concepts in risk management.

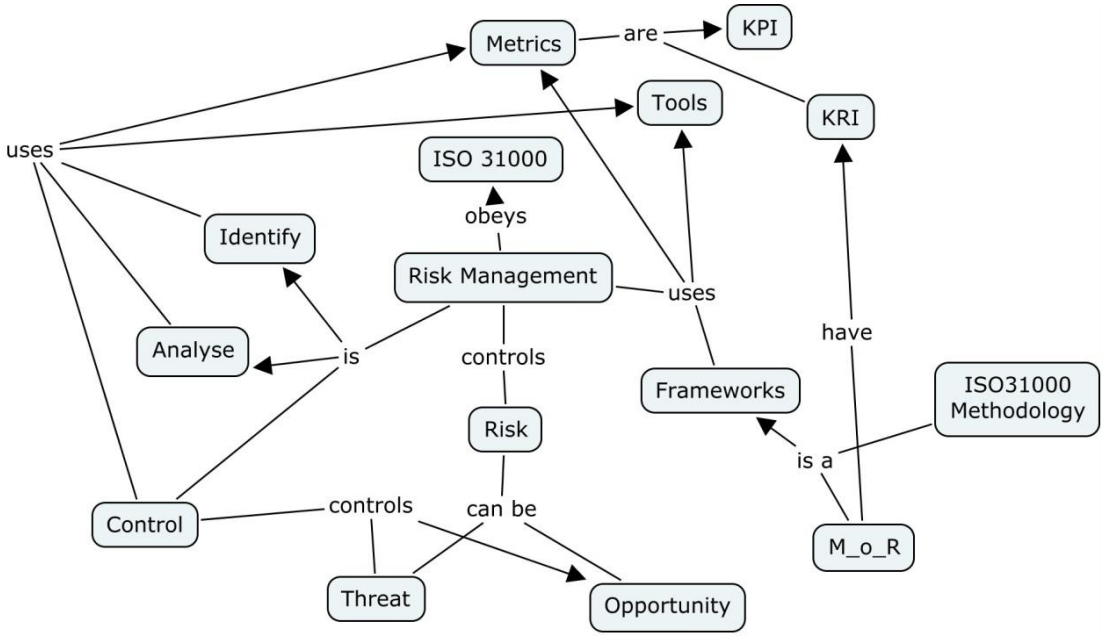

Fig. 6. Risk Management Conceptual Map.

2.4. ITIL

As previously mentioned, ITIL is considered a framework of Best Practice guidance for IT Service Management and is widely used in the business world, not only for IT governance, but for governance in general. A third version was released in July 2007 as an upgrade from version 2, published in 2000. ITIL is a set of guidelines that specifies what the best way to manage IT is. These base lines specify the processes needed in defining, planning, implementing, executing, monitoring and continual improvement of service IT management. In sum, ITIL is a framework based on a service Lifecycle.

A service is something that provides something of value to customers. According to ITIL, all businesses are dependable from the IT Services and the organizations have the duty to provide the best possible quality of service (QoS) to their customers (Office of Government Commerce, 2007).

The ITIL Service Lifecycle includes (in this order):

- **Service Strategy** (21) that understands who the IT customers are, the services that are required to meet the customers' needs and the IT capabilities and resources required to develop a strong organization. This is the part of the cycle in charge of risk management;

- **Service Design** (22)assures that new services and changes to existing services are designed effectively in order to meet customer expectations;
- **Service Transition** (23) this is the phase that ensures customers achieve their goals. In this phase there are actions to:
    - Chang and move systems;
    - Validate;
    - Test;
    - Adapt the employees and customers to the environment.
- **Service Operation** (24) delivers the service on an ongoing basis, daily overseeing its overall health. This includes managing disruptions to service through rapid restoration of incidents, determining the root cause of problems and detecting trends associated with recurring issues, handling daily routine end user requests and managing service access;
- **Continual Service Improvement** (25) involves the Service Lifecycle mechanism for IT to measure and improve the service levels, the technology and the efficiency and effectiveness of processes used in the overall management of services.

Below we can see de ITIL lifecycle with the main activities:

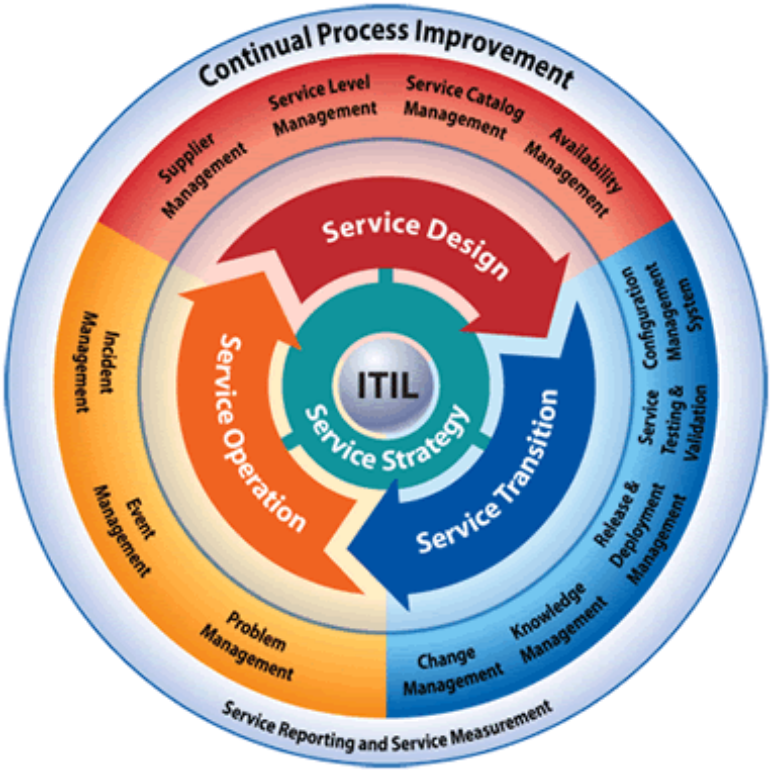

Fig. 7. ITIL v3 2007 lifecycle. Source: http://www.processcatalyst.com/images/itil_v3.gif .

Consistent, repeatable processes are the key to efficiency, effectiveness and the ability to improve services. These consistent, repeatable processes are outlined in the ITIL framework (26).

As a result, ITIL provides several benefits to organizations (27), such as:

- Reduced process costs in the organization;

- Improved IT services through the use of proven best practice processes;
- Improved user and customer satisfaction with IT Services;
- Financial savings from reduced rework, lost time, improved resource management and usage;
- Improved decision making and optimized risk;
- Improved productivity;
- Improved use of skills and experience;
- Framework independent of the platform, technology or business dimension (the described process are generic).

All these benefits are forcing the organizations to enroll in ITIL implementation in order to optimize their IT services and align them with business.

However, sometimes all benefits come with misunderstandings, such as:

- Difficulty in implementing ITIL (28)- As a generic framework ITIL does not have a guide on how to implement risk management. It is important for the implementing organizations to have a well-defined services catalogue. Another possible technique may be to implement ITIL gradually, using a phased approach, and improving the quality of the services gradually;
- Even though ITIL could reduce the cost of the operational process in the organization, it can be costly to implement, and buying all the books for the employees can be prohibitive.
- Another disadvantage lies on the difficulty to estimate the ROI of ITIL implementation (29);
- Organization must adapt to ITIL - staff should change their behaviors based on ITIL (30), this can difficult adapting to the framework.

Although the academic community has been slow to research the phenomenon of multiple framework adoption, some consultants and vendors (such as Borland) have recognized the opportunity to reduce its complexity by providing services related to multiple frameworks. In addition, studies show that the combination of several frameworks empowers the organization (16) (26).

ITIL does not stand alone in providing guidance to IT managers and the Operation Service Book (24) appendices outline some of the key supplementary frameworks, methodologies and approaches that are commonly used in conjunction with ITIL.

2.4.1. ISO20000

Although ISO/IEC20000, like its BS 15000 predecessor, was originally developed to reflect the best practice guidance contained within ITIL, it equally supports other IT Service Management frameworks and approaches (31). It is subdivided in the ISO/IEC 20000-1 and the ISO/IEC 20000-2. While the ISO 20000-1 contains the “Specification for Service Management”, ISO 20000-2 specifies the “Code of practice for Service Management”, describing the best practices as well as the requirements of Part 1.

This Standard has advantages (2008) such as the reputation that it brings to the organization, formality and trusted techniques, which altogether bring a competitive advantage to the organization (List of all benefits in (2008)).

The relationship between ITIL and ISO 20000 is illustrated in the picture below:

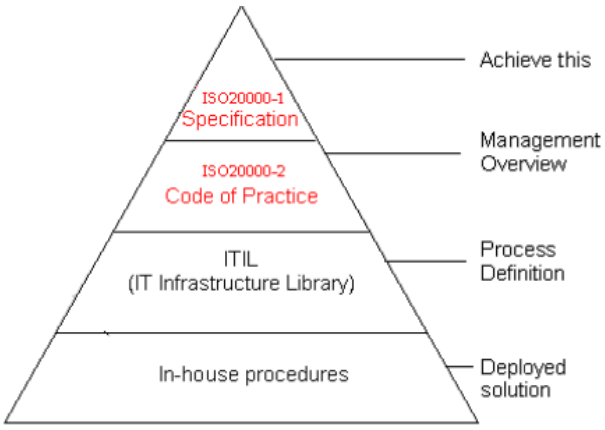

Fig. 8. Relationship between ISO 20000, ITIL and procedures.

As we can see in the picture above, ITIL sustains the ISO 20000 principle, offering a detailed collection of best practices.

2.4.2. ITIL Conceptual Map

We have made a conceptual map with ITIL's main concepts, based on the information available in actual literature:

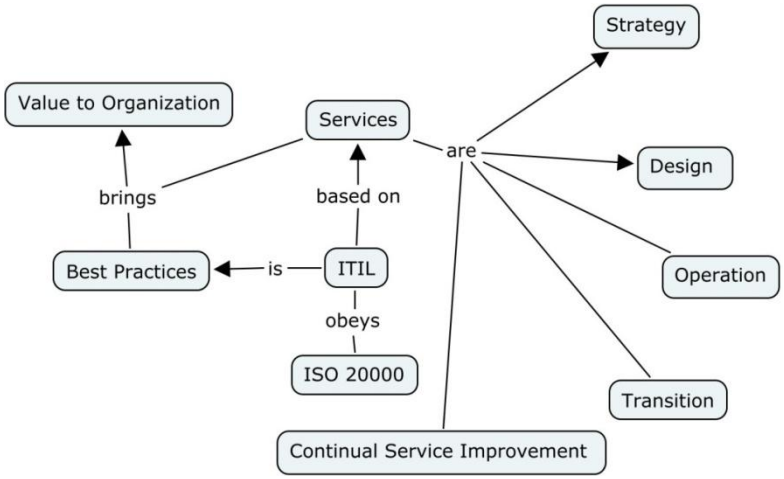

Fig. 9. ITIL Conceptual Map.

2.4.3. Risk Management and Corporate Governance

According to *Essential of Risk* (2), in complex risk-taking organizations, it is not really possible to separate best-practice risk management from best-practice corporate governance. Throughout history, many fatal risks in organizations are associated with business strategies. However, limited or nonexistent interoperability of methods and integration with corporate governance are still a reality (3).

There are some IT governance frameworks that incorporate some elements of risk management already, such COBIT and OCTAVE (3).

Risk in ITIL

ITIL Version 3 highlights the importance of managing corporate risk. While the Service Strategy (21) book and Continual Service Improvement (22) book define what risk and risk management are, the Service Operation (24) book defines how risk is integrated in ITIL.

In the Continual Service Improvement book (22) there is an attempt to clarify what risk management means in ITIL. According to this publication, risk management should take place during the design and transition stages of the service lifecycle. Yet, in this book, it is argued that a good Continual Service Improvement (CSI) program will assess the results of Risk Management activities to identify service improvements through risk mitigation, elimination and management. In order to achieve this, the authors suggest the use of a SWOT analysis. It is important to define mitigation strategies for the risks and to identify the best way to overcome the challenges that an organization may encounter. Knowing the critical success factors before undertaking CSI implementation will be helpful in managing the risks and challenges.

In the Service Operation book (24) every activity has a sub-section with some well-known risks, (Section Challenges, Critical Success Factors and risks subsection risk).

Besides ITIL Books, there are some publications from OGC that deal with Risk and ITIL.

According to OGC, risk management covers the following processes in ITIL (32):

- **Problem management** → there is a proactive and reactive management, with the goal of reducing the impact of service outages;
- **Change management** → Good change management techniques and approaches help reduce risks, minimize the potential negative impact of change, and reduce the risk of an undesirable outcome;
- **Service delivery** → Services must be maintained, so it is important to have a careful design;
- **Availability management** → Focuses on reliability and putting in place alternative options to ensure the service continues;
- **IT service continuity** → Assessing risk to ensure overall continuity for the business.

Daniel Deusing(33) presents an insight to the set of published best practices by the ITIL, the interaction among the ITIL, the Content Management Database (CMDB) and the Risk Management.

The author starts by stating that data is the most important asset to be protected in by IT. Data must be confidential, available, have integrity and be authentic.

In this paper the importance of the association between risk management and the SLAs (***Service Level Agreement***) is also recognized. A well-organized and well-functioning ITSM is a good improvement for better quality, economy and efficiency. The fact that ITSM is responsible for the SLAs makes the ITSM an important factor in Risk Management (34).

The author also suggests a set of guidelines about how to implement risk management in ITIL. The following steps are based on the 10-steps of ITIL Implementation, which is based on the central requirements of the ISO 20000 standard.

- **Step 1:** Exact recognition of the configuration items (CIs) → Inventory analysis of currently available and necessary items required and its implementation in the CMDB;

- **Step 2:** ITIL Project Preparation → Defines the responsibilities, roles and planning (quality, goals and budget);
- **Step 3**: Definition of the IT Service Structure → Organization clarifies what the customer needs, wants to get and what the business company itself should offer to ensure a Service Support to the customer needs;
- **Step 4:** Selection of ITIL Roles and Role Owners → In this step the future owner and the employees of these processes will be determined;
- **Step 5:** Analysis of As-Is Processes: ITIL Assessment / ITIL Self Assessment → Analysis of the current processes' weakness points. With this analysis result it is possible to decide whether to maintain, improve or eliminate the processes;
- **Step 6:** Definition of the To-Be Process Structure → This step is useful to determine the process and sub-process structure;
- **Step 7:** Definition of ITIL Process Interfaces → This step describes the relationship between the processes and what to expect from them;
- **Step 8:** Establishing ITIL Process Controlling → The Process Controlling ensures compliance between the processes provided and the expectations about these processes;
- **Step 9:** Designing the ITIL Processes in Detail → Going deeper in the design of the process;
- **Step 10:** Minimize risk→ In this step precautions are taken against internal and external threats;
- **Step 11:** Selection and Implementation of Application Systems → After this process changes to the IT Infrastructure may be necessary;
- **Step 12:** ITIL Process Implementation and Training.

This is just an example of guidelines regarding ITIL risk management implementations (additional guidelines can be found in IT maps (10) and Deusing's work (35), for instance). The major problem of all these is that they aren't complete and sufficiently integrated into ITIL. Ideally this type of guidelines would be formally included in ITIL rather than being proposed several times by different ITIL users and experts. In the remainder of this dissertation we will approach the problem of defining a complement to ITIL that is responsible for risk management rather than the use of another risk management framework to deal with risk management in IT service management.

2.5. Summary

Unfortunately, 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(35) (37).

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 (36). 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 (36), 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? (37) 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. 2. Risk management coverage according to OGC and critical analysis.

In Wickboldt's article (37), 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.

Despite all these suggestions being valid and useful it would be desirable to have a standard risk management component for any organization (incorporated in ITIL) that didn't force any ITIL user to the use of a second framework for risk management.

3. Model Proposal

In this section we outline our proposed model to simplify and clarify the implementation of risk management in organizations, proposing some new elements of risk management inside ITIL process and making risk management possible in ITIL without using an extra framework to do this.

3.1. Proposal Core

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.

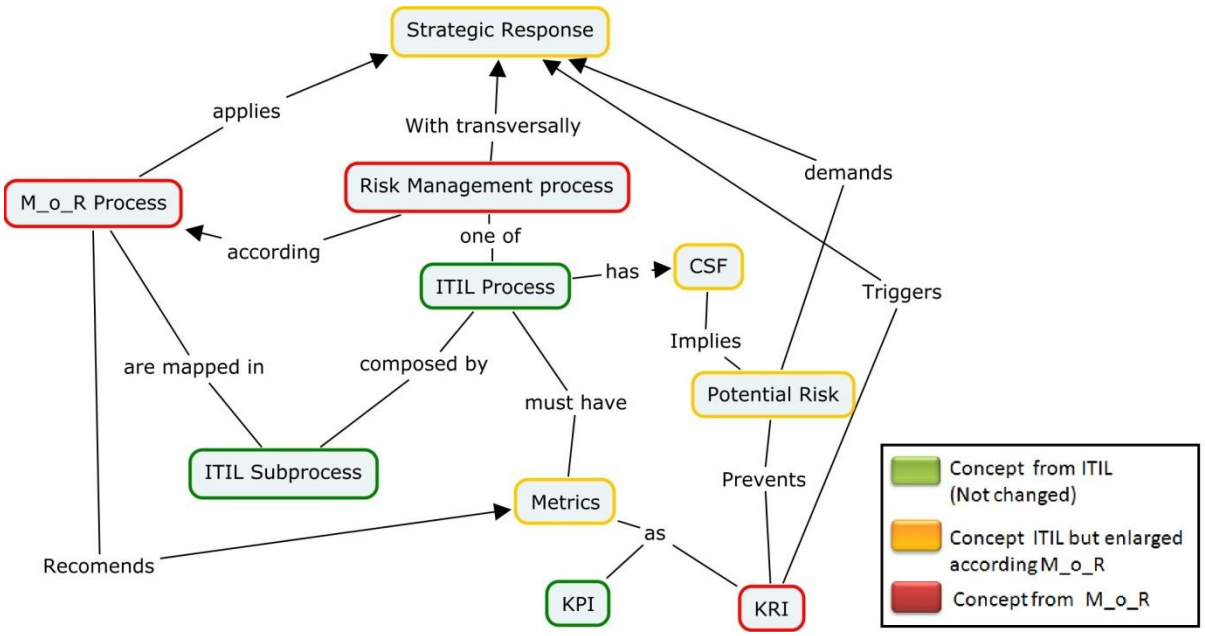

Fig. 10. Model Conceptual Map

To sum up this model combines a set of concepts from ITIL (outlined in green in the conceptual map above), from M_o_R (outlined in red) and concepts shared by these two frameworks (outlined in yellow). 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.

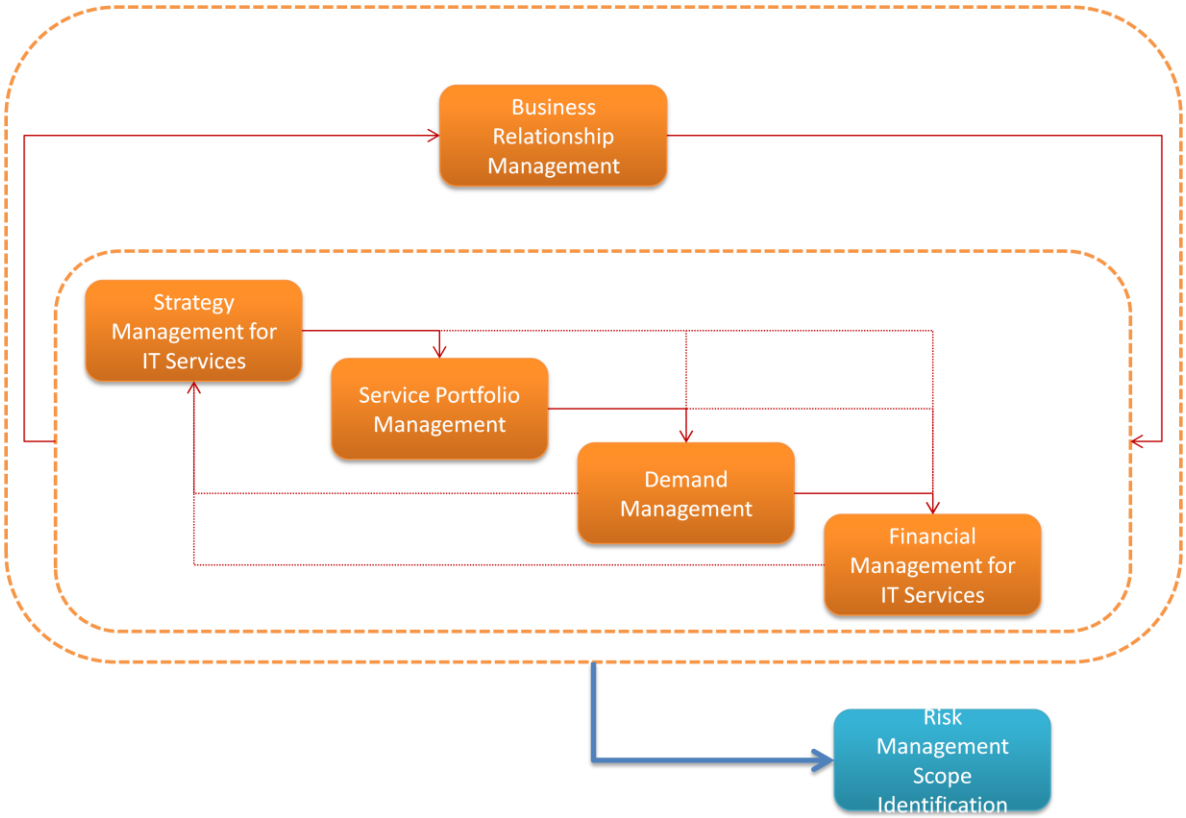

Fig. 11. First Part of Risk Management Process on Service Strategy

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.

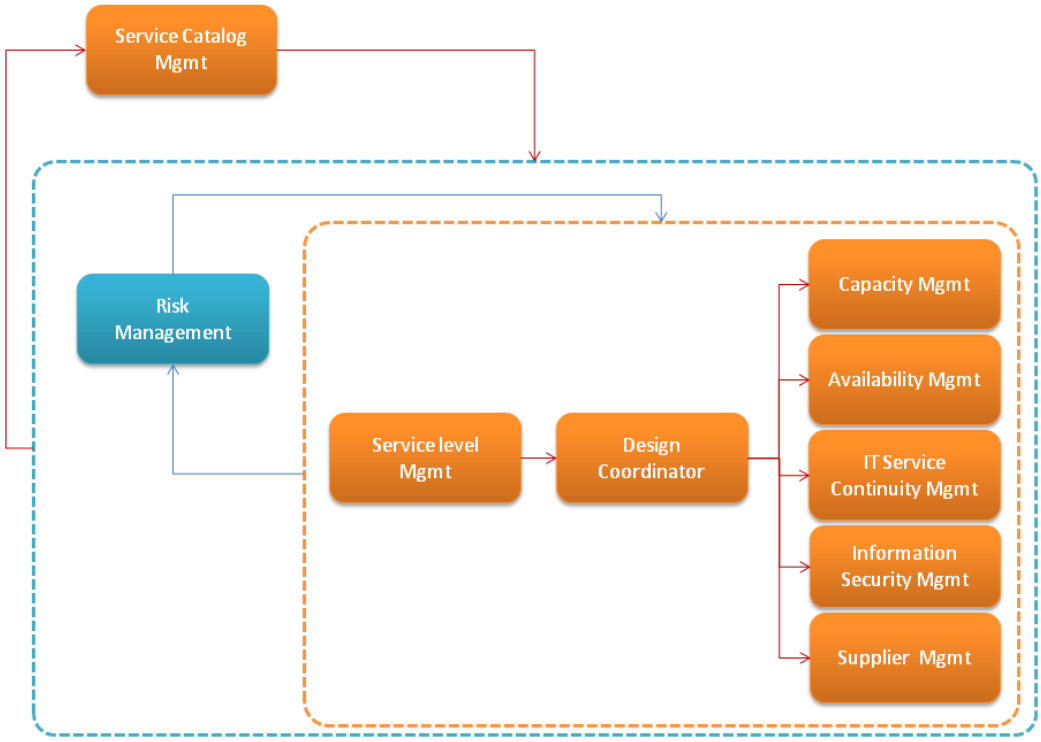

Fig. 12. Second Part of Risk Management Process on Service Design

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 (10). 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).

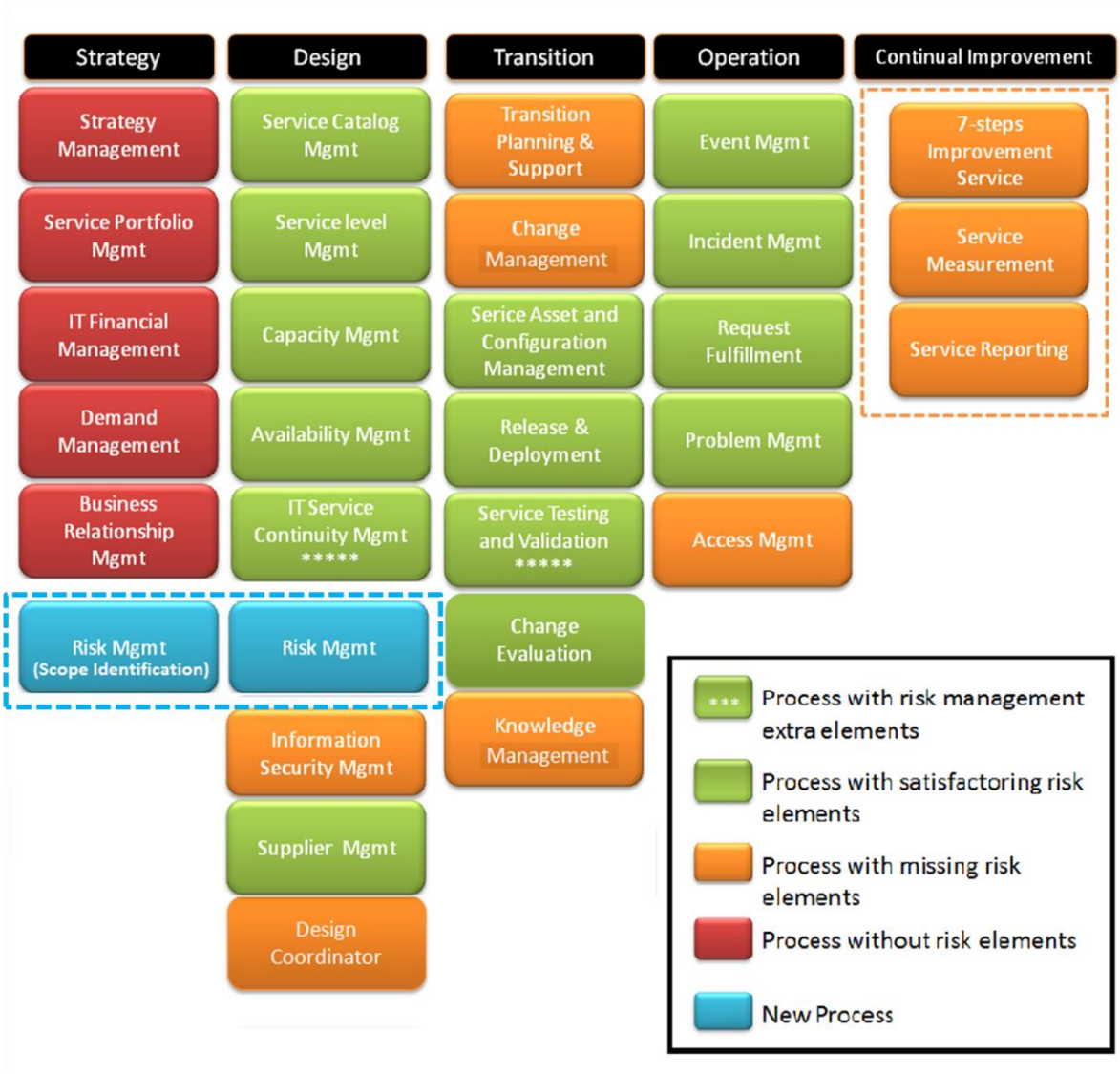

Fig. 13. ITIL Process Map According Risk Elements Plus New Process

In figure 13 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.

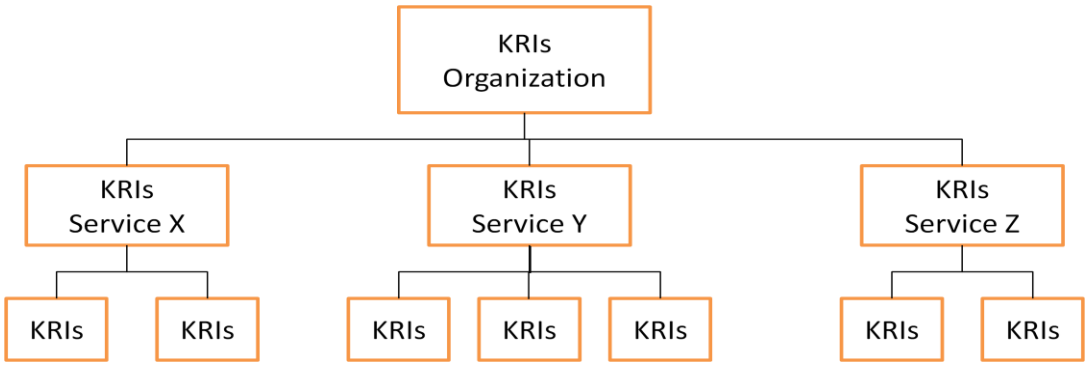

Fig. 14. Work breakdown structure of KRIs

This KRIs must be defined from top to bottom according 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. Following we presents a example of ITIL process mapped with M_o_R process:

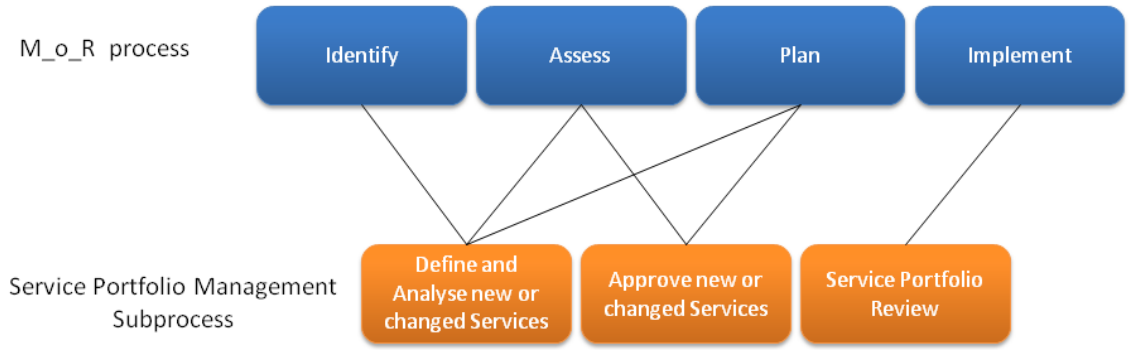

Fig. 15. Example M_o_R process Mapped to ITIL sub-process.

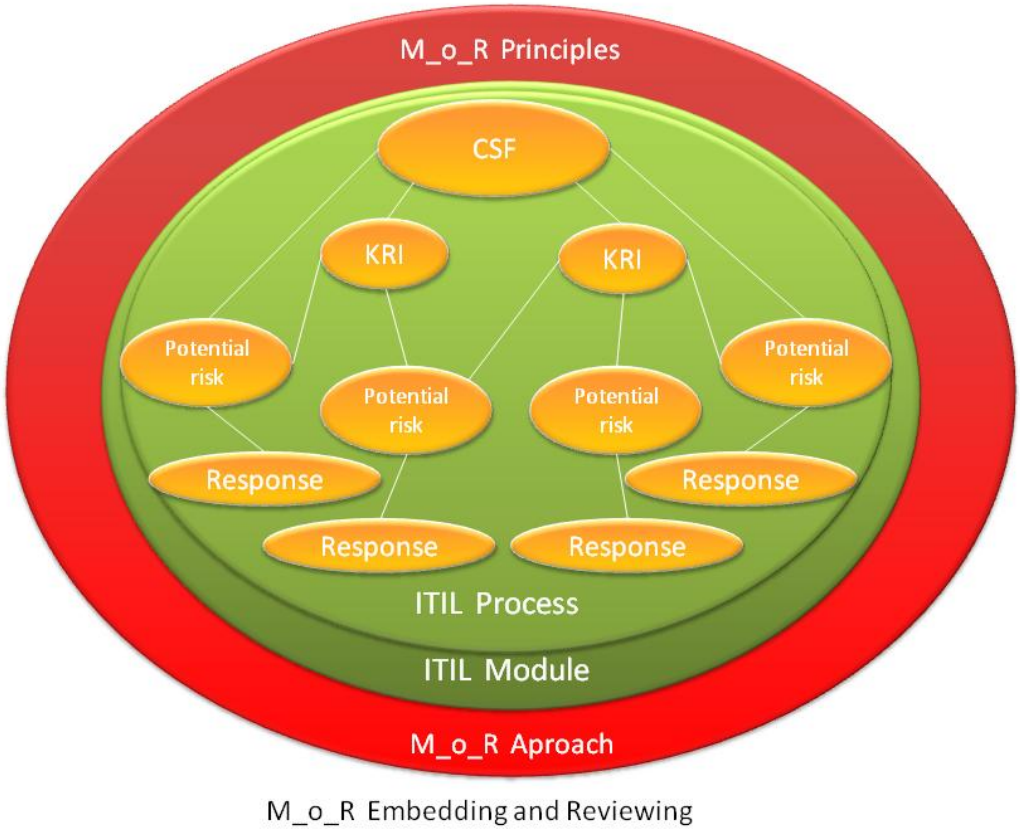

Fig. 16. Mapping of M_o_R Concepts in ITIL

The M_o_R concepts (KRI's, strategic response, potential risks) are mapped inside ITIL processes. But for all working its important wrap one by one ITIL (going to ITIL subprocess) process by M_o_R principles and approach. In accordance to M_o_R, there are 8 principles (see section 2). Although this is a useful and complete set of guidelines about what is expected from a risk management framework in an organization, according to ISO31000, there are some gaps. One of them is the fact that opportunity is not referred to, like in M_o_R.

M_o_RThese 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 transversal way in all ITIL Process.

Wrapping all ITIL processes, M_o_R concepts of embedding and review must be integrated in CSI. The values 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.

For more detail on this topic see Section 3.6 Continual Service Improvement.

Next we systematically apply this model to ITIL process. Hence the chapter structure follows the ITIL structure. Each section corresponds to an ITIL module and each sub-section corresponds to an ITIL process containing:

- A summary about the process and its relationship with risk management;
- Its critical success factors (CSF);
- A table with its main potential risks, KRIs and strategic response;
- A mapping of M_o_R processes on each sub-process ITIL.

3.2. Service Strategy

The strategy services are mostly about identifying all the organization's scope, including risk. Service Strategy process determines which services the IT organization offers and what capabilities need to be developed.

The risk part is about the ability of the organization to limit its exposure to risk. The aim should be to make an accurate risk assessment in a given situation, and analyze the potential benefits.

3.2.1. Strategy Management for IT Services

The objective of Strategy Management for IT Services is to assess the service provider's offerings, capabilities, competitors as well as current and potential market spaces in order to develop a strategy to serve customers. Once the strategy has been defined, ITIL Strategy Management is also responsible for ensuring the implementation of the strategy(21).

The risk management steps assigned to its sub-process are:

- **Identify** and **Assess** on Strategic Service Assessment;
- **Identify** and **Plan** on Service Strategy Definition;
- I**mplement** on Service Strategy Execution.

To achieve these processes' goals, the Critical Success Factors identified are:

- To define a structured and competitive strategy;
- To implement the defined strategy.

The potential risk and KRIs for this are:

Potential Risk	KRI (Key Risk Indicators)	Strategic Response
Define a not structured or competitive strategy.	Decrease/Increase of customers satisfaction.	Define and document organization‘s goals, important input from clients and external service providers in a, for instance, strategy plan. Create Strategic Action Plan defining specific tasks and responsibilities.
Creation of a service that is not aligned with organization strategy or organization/customer.	Decrease /Increase of customers. Rate of service utilization.	Analyze the impact on existing services, create new services in the organization and determine the assets required to offer the service.
Customer number variation.	Decrease /Increase of customers.	Determine the amount max and min of customers to provide a service (costs, profits). Elaborate a plan in case of customer variation, while controlling the amount of customers through lists, reports and proper documentation (according to M_o_R recommendations).

Table. 3. Potential risks, KRIs and Strategic Response for SMITS.

3.2.2. Service Portfolio Management

Service Portfolio Management is all about managing 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(21). The risk management steps assigned to its sub-process are:

- **Identify**, **Assess** and **Plan** on Defining and Analyzing 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 fit customer necessities;
- Determine the capability of services and adjust it according to the number of customers;
- 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 aligned with the organization‘s strategy or organization/customer.	Decrease/Increase of customers satisfaction. Decrease /Increase of customers.	Analyze the impacts on existing services and the creation of new services in the organization and determine the assets required to offer the service.
Customer number variation.	Decrease /Increase of customers. Rate of service utilization.	Determine the amount max and min of customers to provide a service (costs, profits). Elaborate a plan in case of customers variation. Controlling the amount of customers through lists, reports and proper documentation (according to M_o_R recommendations).
Not keeping the Service Portfolio up-to-date.	Number of services registered in the services portfolio. Frequency of activity on the Service Portfolio.	After approved the service must be formally identified in the Service portifolio and communicated to organization. Creation of a Service Portfolio Review Report, a document containing the results and findings from a Service Portfolio Review.

Table. 4. Potential risks, KRIs and Strategic Response for Service Portfolio Management.

3.2.3. Demand Management

Demand Management aims to understand, anticipate and influence customer demand for services. Demand Management works with Capacity Management to ensure that the service provider has sufficient capacity to meet the required demand(21). The risk management steps are all made in Demand Management without sub steps.

The Critical Success Factors are:

- Understand customer needs;
- Determine the capacity of satisfying customers.

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

Potential Risks	KRI (Key Risk Indicators)	Strategic Responses
Not identify customer demands for services.	Number of services with good feedback. Decrease / Increase of customer.	Study customer needs (surveys, questionnaires, observation).
Being unable to determine the optimal capacity to meet customer needs.	Ratio of services demanded by customers by services delayed/not satisfied .	Study customer needs (surveys, questionnaires, observation). Conduct performance tests before exposing customer to services.

Table. 5. Potential risks, KRIs and Strategic Response for Demand Management.

3.2.4. Financial Management for IT Services

The objective of this process is to manage the service provider's budgeting, accounting and charging requirements(21). The risk steps are enrolled in its sub-process as following:

- **Identify** on Financial Management Support;
- **Identify, Assess and Plan** Financial Planning;
- **Assess and Plan** on Financial Analysis and Reporting;
- **Implement** on Service Invoicing.

Critical Success Factors:

- Plan a structured budget plan;
- Estimate a good deal of Cost/benefits.

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

Potential Risk	KRI (Key Risk Indicators)	Strategic Response
Plan Incorrect Budget.	Percent of IT expenses exceeding approved budget.	Ensure and compare budget available with budget necessary. Identify and elaborate a list of the most essential elements in strategy and start cutting down to up. Define necessary structures for management of services cost (Create documentation such as budget request, budget allocation).
Inaccurate Cost / Benefit Estimation.	Ratio of projects/benefits verified after implementation of strategy. Percent of profit per service.	Define necessary structures for the management of financial planning data.

Table. 6. Potential risks, KRIs and Strategic Response for FMITS.

3.2.5. Business Relationship Management

The Business Relation Management objective is to maintain a positive relationship with customers. Business Relationship Management identifies the needs of existing and potential customers and ensures that appropriate services are developed to meet them(21). The M_o_R process mapping for management of risk in this process is:

- **Implement** on Maintain Customer Relationships;
- **Identify, assess and plan** on Identify Service Requirements;
- **Identify** on Sign up Customers to Standard Services;
- **Identify, assess and plan** on Customer Satisfaction Survey;
- **Assess** on Complaints Management.

The main Critical Success Factors are:

- Maintain a positive relationship with customers;
- Identify the needs of existing and potential customers.

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

Potential Risk	Key Risk Indicator	Strategic response
Not satisfying customers, resulting in complains or reduction of customers.	Number of received complains. Number of customers. Percentage of returned questionnaires.	Analyze the source of complaints and determine which ones are acceptable according to services contract (previous agreement with customers). Maintain Information about the complaints (Complaint Status Information, Complaints and Compliments, Complaints Log and so on). Send surveys questionnaires and know customer's opinion about services offering.
Not receive significant Feedback of services.	Percentage of returned questionnaires. Number of received complaints. Customer Satisfaction per Service.	Elaborate short simple questionnaires. Let customers know that the feedback will be used (communicate changes provided by questionnaires' results). Send survey questionnaires and find out customer's opinion about services offering. Maintain Information about the complaints (Complaint Status Information, Complaints and Compliments, Complaints Log and so on).

Table. 7. Potential risks, KRIs and Strategic Response for Business Relationship Management.

3.2.6. Risk Management

The risk management process is not in the original ITIL Framework. However, it would be extremely useful as a process responsible for managing risk, according M_o_R guidelines.

In this model we choose split the risk process in two parts: One present in service strategy, and other in the service design.

The first phase of risk management process is responsible for identifying what risks the organization is willing to take. It is in this phase that the achievable CSFs are defined. So risk management receives output from the other service strategy processes and defines the limits of risk in the organization. It is the accountability part.

The risk management process is explained as a whole process is explain in Design Risk Management on section 0

3.3. Service Design

The scope of Service Design includes the design and development of new services as well as changes and improvements to existing ones. It covers design principles and methods for converting strategic objectives into services and service assets. These principles must be in accordance with M_o_R principles.

There are a number of risks directly associated to the Service Design phase of the Service lifecycle. These risks need to be identified, assessed, planned and implemented to ensure that they receive proper treatment.

But this is not enough for a good risk management. A good implementation of the new process**,** the **Risk Management process**, is important. The objective of the Risk Management process is to

identify, assess and control risks. This includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats.

Following we will identify the key risk indicators of all Design Processes and detail the new **Risk management process.**

3.3.1. Design Coordination

The Design Coordination process objective is to coordinate all service design activities, processes and resources. Design coordination ensures the consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information and metrics(35). The M_o_R process mapping for management of risk is:

- **Identify, Assess** and **Plan** on Design Coordination Support;
- **Assess** and **Plan** on Service Design Planning;
- **Identify, Assess, Plan** and **Implement** on Service Design Coordination and Monitoring;
- **Identify, Assess** on Technical and Organizational Service Design;
- **Implementation** on Service Design Review and RFC Submission.

Critical Success Factors:

- Coordinate all service design activities, process and resources;
- Ensure consistent and effective design.

Potential Risk	Key Risk indicator	Strategic Response
No coordination of interrelated services.	Number of Resources. Number of services related. Number of service links.	Create a web of services. Create a list with all services and their supposed goals.
Not achieve the consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information and metrics.	Number of services related.	Create a service design policy specifying which projects or changes are required to undergo the formal Service Design stage, and who needs to be involved in Service Design to ensure that all relevant aspects are considered. Specifies the requirements from the client‘s viewpoint and defines how these are actually fulfilled from a technical and organizational point of view.

Table. 8. Potential risks, KRIs and Strategic Response for Design Coordination.

3.3.2. Service Catalogue Management

The Service Catalogue Management Process objective is to ensure that a Service Catalogue is produced and maintained, containing accurate information on all operational services and those being prepared to be run operationally. Service Catalogue Management provides vital information for all other Service Management processes: service details, current status and the services' interdependencies(35). There is no sub-process.

The main Critical Success Factors for the Service Catalogue Management process are:

- An accurate Service Catalogue;
- Business users’ awareness of the services being provided;

- IT staff awareness of the technology supporting the services.

So the potential risks, KRIs and strategy responses are:

Potential Risk	Key risk Indicator	Strategy Response according M_o_R
Inaccuracy of the data in the catalogue	Frequency of activity on Service Catalogue.	Document all changes in a log and immediately communicate the changes to stakeholders (Put in strict change control). The service Catalogue must contain the details and the current status of every live service provided by the service provider or service being transitioned into the live environment, together with the interfaces and dependencies.
Poor acceptance of the Service Catalogue and its usage in all operational processes.	Frequency of activity on the Service Catalogue. Catalogue evaluation by stakeholders.	The more active the catalogue is, the more likely it is to be accurate in its content. The service catalogue must contain the details and the current status of every live service provided by the service provider or service being transitioned into the live environment, together with the interfaces and dependencies.
Poor quality of tools and resources.	Number of complaints about tools. Experts evaluation about tools. Percentage of users actually using the tools.	Keep inventory of tools and resources that are needed and available. Maintain backup tools and a suppliers' channel.
Poor access to accurate Change Management information and processes.	Number of access to documents. Number of documents update.	Document all changes in a log and immediately communicate the changes to stakeholders. Keep catalogue service accurate and updated in its content.
Poor access to and support of appropriate and up-to-date CMS and SKMS.	Number of access to documents.	Keep a database or structured document with information about all live services, including those available for deployment. The Service Catalogue is the only part of the Service Portfolio published to customers, and it is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request processes.
The information is either too detailed to be accurately maintained or at too high a level to be of any value.	Number of access to documents.	Have documentation as short as possible. Have documentation specifying more than one level of detail (one for users, one for support, and so on).

Table. 9. Potential risks, KRIs and Strategic Response for Service Catalogue Management.

3.3.3. Service Level Management

Service Level Management (SLM) negotiates, agrees and documents appropriate IT service targets with representatives of the business, and then monitors and produces reports on the service provider's ability to deliver the agreed level of service(35). The M_o_R process mapping for management of risk is:

- **Plan** and **Implement** on Maintenance of the SLM Framework;
- **Identify** and **Assess** on Identification of Service Requirements;
- **Implement** on Agreements Sign-Off and Service Activation;
- **Implement** on Service Level Monitoring and Reporting.

The main CSFs for the Service Catalogue Management process are:

- Manage the overall quality of IT services required;
- Deliver the service as previously agreed at affordable costs;
- Manage the interface with the business and users.

Potential risks, KRIs and strategy responses are in table 10 following.

Potential Risk	Key Risk Indicator	Strategic Response
A lack of accurate input, involvement and commitment from the business and customers.	Number of customers willing to give feedback about services.	Engage customers to involve and commit in creation of services (showing the benefits of suggestions, critics, giving them advantages if participates).
The tools and resources required to agree, document, monitor, report and review agreements and service levels are not adequate.	Number of complaints about tools. Experts evaluation about tools. Percentage of users actually using the tools.	Estimate with experts the necessary tools for document, monitor, report and review service levels. Create a politic encouraging their use and knowledge.
The process becomes a bureaucratic, administrative process rather than an active and proactive process, delivering measurable benefit to the business.	Number of process/steps and their time of each step.	Be attention for do not extend the process. See with experts if process can be shorted or simplified.
Innappropriate access to and support of up-to-date CMS and SKMS.	Number of access to documents.	Define appropriated services and service portfolio. Keep a database or structured document with information about all live services, including those available for deployment. The Service Catalogue is the only part of the Service Portfolio published for customers, and it is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request processes.
Bypassing the use of the SLM processes.	Times of bypassing the use of the SLM processes.	Show the advantages of following SLM. Disapprove the non-following of SLM process (censure, sanctions and so on).
Business and customer measurements are too difficult to determine and improve, so they are not recorded.	Business elements that can be measured.	Search for the easiest way to record measurements (appropriate financial and IT management tools instead of just using Excel).
Inappropriate behavior of the organization's staff.	Number of complaints due to staff behavior.	Develop a set of appropriate behaviors for the organization's employees. Incentive contacts through organization channels.
Customer expectations do not match reality and there is a low perception of what services can provide.	Number of misunderstandings in communication.	Previous agreement between organization and customers about services outputs. Document appropriate service outputs, and monitor the service performance.
Poor and inappropriate communication is achieved in the business and with customers.	Number of change requests resulting from functionality "not satisfied by the organization".	Develop a set of appropriate behaviors (behavior guidelines) for the organization's staff. Encourage contacts through organization channels. Be clear in objectives, expectations, and capacity in documentation. Develop a set of appropriate behaviors for organization people. Incentive contacts through organization channels.

Table. 10. Potential risks, KRIs and Strategic Response for Service Level Management.

3.3.4. Capacity Management

The Capacity management process is responsible for ensuring that the capacity of the IT services and IT infrastructure are able to deliver the agreed service level targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT service, and plans for short, medium and long term business requirements(35). There are many risks associated to this process. The M_o_R mapping process structure is:

- **Plan on** Business Capacity Management;
- **Implement on** Service Capacity Management;
- **Implement on** Component Capacity Management;
- **Implement on** Capacity Management Reporting.

The main Critical Success Factors for the Capacity Management process are:

- Accurate business forecasts;
- Knowledge of current and future technologies;
- Ability to demonstrate cost-effectiveness;
- Ability to plan and implement the appropriate IT capacity to match business needs.

Potential risks, KRIs and strategy responses are in table 11 following:

Potential Risk	Key Risk Indicator	Strategic Response
Poor commitment from the business to the Capacity Management process.	Incidents due to Capacity Shortages. Exactness of Capacity Forecast. Percentage of Capacity Monitoring.	Do not commit beyond organization capacity. Create documentation, registering capacity qualities agreed upon with customers such as: - Capacity Management Information System, a virtual repository of all Capacity Management data, usually stored in multiple physical locations. - Capacity Plan, used to manage the resources required to deliver IT services. The plan contains scenarios for different predictions of the business demand, and costly options to deliver the agreed service level targets. - Capacity Report providing other Service Management processes and IT Management with information related to service and resource use and performance.
Lack of appropriate information from the business on future plans and strategies.	Number of elements with relevance for business documented. Incidents due to Capacity Shortages.	Register and document the main aspects of business (policies, techniques, scope, so on), i.e. everything essential to achieve organization goals.
Lack of senior management commitment or a lack of resources, and/or budget for the Capacity Management process.	Number of resources compromised due to lack of budget. Incidents result from Capacity Shortages.	Identify the resources/budget necessary for management (see strategy documents).
SCM and CCM performed in isolation because BCM is difficult, or there is a lack of appropriate and accurate business information.	Number of resources compromised due to lack of budget.	Create documentation to help identify the needed budget (see strategy documents).
The processes become too bureaucratic or manually intensive.	Number of process/steps. Time of each step. Incidents due to Bureaucracy. Resolution Time of Capacity Shortage.	Pay close attention not to extend the processes. See with experts if processes can be shorted or simplified. Create an event filter, rules and criteria to determine if an event is significant and to decide upon an appropriate response.
The processes focus too much on technology (CCM) and not enough on services (SCM) and the business (BCM).	Incidents caused by Capacity Shortages.	Pay close attention to not focus the process just on technology. Consult experts to check if processes are focused on customer and not just on delivering the service (as they are not humanized).
The reports and information provided are too bulky or too technical and do not provide the required or appropriate information to the customers and the business.	Number of documentation pages. Number of distinct types of documentation. Effective use of documentation by stakeholders.	Simplify without being basic. Provide several levels of documentation according to the stakeholder‘s profile (users, support, board, and so on). Establish an acceptable number of pages for each documentation, according to experts’ opinion.

Table. 11. Potential risks, KRIs and Strategic Response for Capacity Management.

3.3.5. Availability Management

The availability management goal is to define, analyze, plan, measure and improve all aspects of the IT services' availability. Availability Management is responsible for ensuring that the level of service availability delivered in all services is matched to or exceeds the current and future agreed business needs, in a cost-effective manner(35).

- **Plan, assess and Implement** on Design Services for Availability;
- **Implement** on Availability Testing;
- **Identify, Implement** on Availability Monitoring and Reporting.

The main CSFs for the Availability Management process are:

- Manage availability and reliability of IT service;
- Satisfy business needs for accessing IT services;
- Availability of IT infrastructure, as documented in SLAs, provided at optimum costs.

The risk associated with Availability Management is similar to the risk associated with Capacity Management so the KRI are similar.

Potential risks, KRIs and strategy responses are in table 12 following:

Potential Risk	Key Risk Indicator	Strategic Response
A lack of commitment from the business to the Availability Management process.	Incidents due to poor availability. Percentage of Availability Monitoring. Number of Service Interruptions. Duration of Service Interruptions.	Do not commit beyond organization capacity. Integration of all of the available data into an integrated set of information (AMIS) that can be analyzed in a consistent manner to provide details on the availability of all services and components. Create documentation registering availability qualities agreed with customers, such as: - Availability Design Guidelines, Guidelines that define from a technical point of view how the required availability levels can be achieved, including specific instructions for application development and for externally sourced infrastructure components. - Availability Guidelines for the Service Desk - Rules produced by Availability Management on how to manage incidents causing unavailability to prevent minor incidents from becoming major incidents. - Availability Management Information System, a virtual repository of all Availability Management data, usually stored in multiple physical locations. - Availability Plan with detailed information about initiatives aimed at improving service and/ or component availability. - Recovery plan containing precise instructions for returning specific services and/or systems to a working state, which often includes recovering data to a known consistent state.
Lack of appropriate information on future plans and strategies.	Number of documented elements with relevance for the business. Incidents due to Availability Shortages. Number of Service Interruptions. Duration of Service Interruptions.	Register and document the main aspects of business (policies, techniques, scope, and so on), everything essential to achieve organization goals. Convincing the business and senior management of the investment needed in proactive availability measures.
Lack of senior management commitment or lack of resources and/or budget to the Availability Management process.	Number of Service Interruptions. Duration of Service Interruptions.	Identify the resources/budget necessary for management (see strategy documents).
Reporting processes become very labor-intensive.	Effort for make reporting process. Filter level.	The effort made in the reporting process must be less than that of the process itself. Event Filtering and Correlation Rules used to determine if an event is significant and to decide upon an appropriate response. Create documentation describing the procedures required to run and maintain a type of application or infrastructure component.
AMIS is maintained in isolation and it is not shared or consistent with other	Incidents result from poor availability.	Create a plan linking availability and organization services. Produce documents describing the link between AMIS and

process areas, especially ITSCM, Security Management and Capacity Management.	Documentation produced.	other process. Describe link qualities, method steps and business elements involved. Create redundancy to increase availability.

Table. 12. Potential risks, KRIs and Strategic Response for Availability Management.

3.3.6. IT Service Continuity Management

The goal of IT Service Continuity is to support the overall Business Continuity Management process by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment technical support and Service Desk) can be resumed within required, and agreed on, business timescales. As technology is a core component of most business processes, the continued or high availability of IT is critical to the survival of the business as a whole. This is achieved by introducing risk reduction measures and recovery options(35). Next we can see the M_o_R process mapped on ITSCM sub-process:

- **Implement** on ITSCM Support;
- **Plan and Implement** on Design Services for Continuity;
- **Implement** on ITSCM Training and Testing;
- **Identify, Assess and Implement** on ITSCM Review.

The main Critical Success Factors for the ITSCM process are:

- IT services are delivered and can be recovered to meet business objectives;
- Awareness throughout the organization of the business and IT Service Continuity Plans.

Some of the major risks associated with ITSCM include and its respective KRIs and strategic responses are:

Potential Risk	Key Risk Indicator	Strategic Response
Lack of commitment from the business to the ITSCM processes and procedures.	Gaps in Disaster Preparation. Number of identified shortcomings during Disaster Practices.	Do not commit beyond organization capacity. Register and document the main aspects of business (policies, techniques, scope, and so on), i.e. everything essential to achieve the organization's goals. Create a Business Continuity Strategy, an outline of the approach to ensure the continuity of vital business functions in the case of disaster events.
Lack of appropriate information on future plans and strategies.	Gaps in Disaster Preparation. Duration of the identification of a disaster-related risk to the implementation of a suitable continuity mechanism. Number of identified shortcomings during Disaster Practices.	Register and document the main aspects of business (policies, techniques, scope), i.e. everything essential to achieve the organization's aims. Convincing the business and senior management of the investment needed in risk management measures and recovery plans by presenting experts' analysis and documentation support. Create a Business Continuity Strategy, an outline of the approach to ensure the continuity of vital business functions in the case of potentially disastrous events. Create Disaster Recovery Invocation Guideline.
Lack of senior management commitment or lack of resources and/or budget for the ITSCM process.	Number of service interruptions. Duration of service Interruptions	Identify the resources/budget necessary for management (see strategy documents).
The processes focus too much on technology issues and not enough on IT Services and the needs and priorities of the business.	Number of automated processes.	Pay close attention to not focus process just on technology. Consult experts to check if processes are focused on customer and not just on delivering the service (as they are not humanized .
Risk Analysis and Management are conducted in isolation and not in conjunction with Availability and Security Management.	Number of service interruptions.	Create a relation between availability and risk events, create KRIs. Create tables linking risk management elements. Create Availability/ ITSCM/ Security Testing Schedule, schedule for the regular testing of all availability, continuity and security mechanisms, jointly maintained by Availability, IT Service Continuity and Information Security Management.
ITSCM plans and information become out-of-date and lose alignment with the information and plans of the business and BCM.	Number of updates in plan and information.	Create a documentation update routine. The responsible for updating ITSCM must be the same that updates BCM.

Table. 13. Potential risks, KRIs and Strategic Response for IT Service Continuity Management.

3.3.7. Supplier Management

The purpose of the supplier management process is to obtain value for money from suppliers and to ensure that suppliers perform to the targets contained within their contracts and agreements, while conforming to all of the terms and conditions(35). Following the M_o_R process mapped in Supplier sub-process:

- **Identify, assess, plan** on Providing the Supplier Management Framework;
- **Identify, assess** on Evaluation of new Suppliers and Contracts;
- **Implement** on Establishing new Suppliers and Contracts;
- **Implement** on Processing of Standard Orders;
- **Implement** on Supplier and Contract Review;
- **Implement** on Contract Renewal or Termination.

The Critical Success Factor for Supplier Management is:

- Obtain value for money from suppliers.

Potential risks, KRIs and strategy responses are:

Potential Risk	Key Risk Indicator	Strategic Response
Not obtain value to organization.	Number of agreed UCs. Number of contract reviews. Number of suppliers in the SCMIS and the information about them.	Create Supplier and Contract Management Information System (SCMIS), a database or structured document used to manage suppliers and contracts throughout their lifecycle. The SCMIS contains the key attributes of all contracts with suppliers, and should be part of the Service Knowledge Management System.
Suppliers do not provide expected service.	Number of identified contract breaches. Number of requirements filled in contracts.	Create Standard Terms and Conditions, a set of terms and conditions which are routinely attached to contracts and orders when procuring services or products.
Select not suitable supplier.	Number of identified contract breaches. Number of requirements filled in contracts.	Create a supplier strategy that defines the suppliers qualities, and obligations. Create Standard Terms and Conditions, a set of terms and conditions which are routinely attached to contracts and orders when procuring services or products. Create a supplier evaluation document describing in detail the criteria used for evaluating and selecting a suitable supplier.

Table. 14. Potential risks, KRIs and Strategic Response for Supplier Management.

3.3.8. Risk Management

As a new process, Risk Management has never defined in original ITIL books so here it is written following ITIL books structure like the other processes has written.

Purpose/goal/objective:

The objective of second phase of risk management (see section 3.2.6 the first phase of risk management) is to identify, assess and control risks. This includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats.

Risks are addressed within several processes in ITIL but, there is none dedicated to the Risk Management process. ITIL calls for "coordinated risk assessment exercises" although according to M_o_R, it would be natural to assign clear responsibilities for managing risks, which would mean introducing a specific Risk Management process as part of the ITIL processes.

Below we specify the desirable characteristics of this new process.

Scope:

Risk management must be done transversally to the organization. Its action must be proactive and seek to understand the size of possible threats and opportunities. Risk must be reduced to something that is manageable for the first release and defer the rest for subsequent ones (Something that will not be possible to do until everyone understands what is at stake). For this reason, the risk management process must provide input to other design processes and receive output from them as showed in figures Fig 12.

Value to Business:

Having a basic Risk Management process in place will provide a good starting point for introducing best-practice Risk Management like in M_o_R.

Policies/principles/basic concepts:

The purpose of the risk management policy is to communicate why and how risk management will be implemented throughout an organization (or part of an organization) in order to help accomplish its objectives.

Although a hierarchy of policies is often adopted, it is also valid for a large organization to have a single risk management policy that applies to all organizational activities.

The risk management policy should be reviewed and updated at least once a year after the release of new legislation or government guidance affecting corporate governance, internal controls, financial management or relevant regulatory regimes for the sector.

Sub-process:

The sub process of risk management second phase (service design risk management) are based on IT Maps (10).

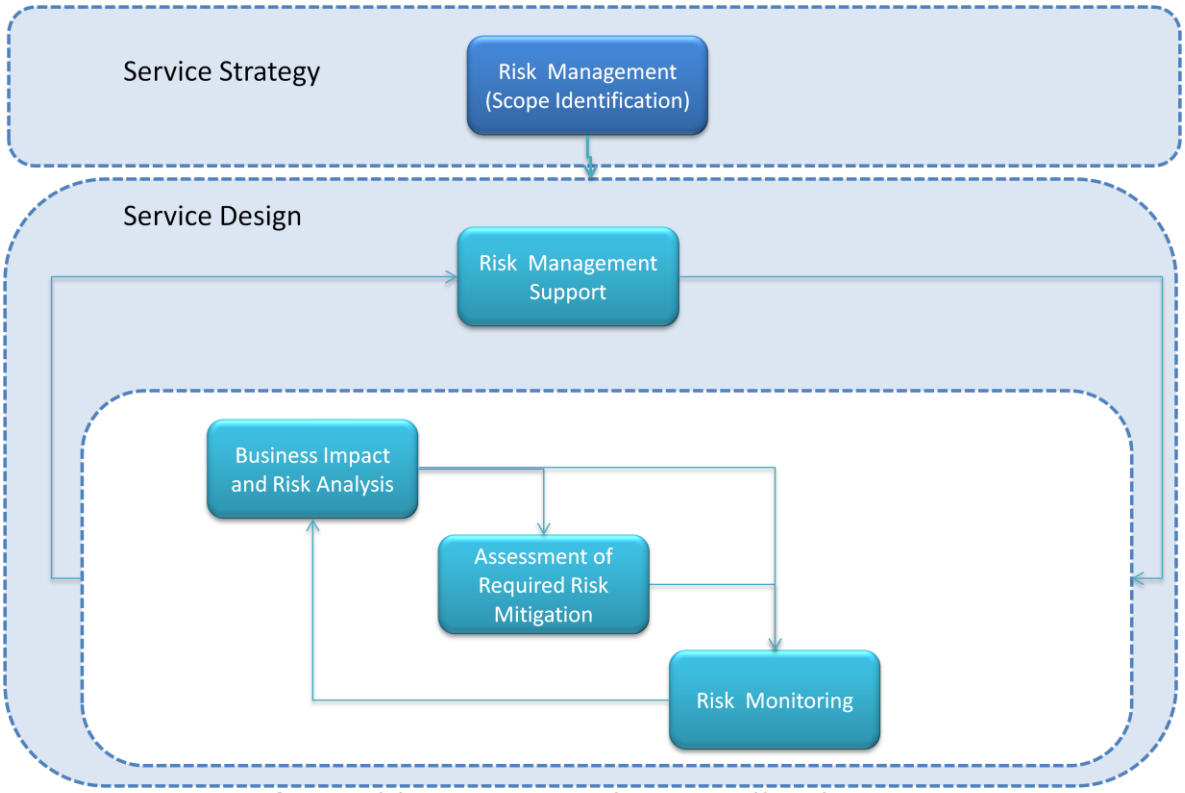

Fig. 17. Risk Management Sub-process Lifecycle.

- ***Risk Management Identify Scope (on Service Strategy)***

  This sub-process (the first phase of risk management) is responsible for providing the organization with the bases of risk management. This phase receives output from strategy services and provides guidelines about what risks organization can or cannot support and for creating or nominating who is in charge of the various Risk Management duties. This phase produces the boundaries and the main CSF.

- ***Risk Management Support:***

  This is the sub-process responsible for identifying risks after a service's strategic definition. Its goal is to define a framework for Risk Management based on the limits imposed by risk management on Service Strategy.

- ***Business Impact and Risk Analysis:***

  This sub-process' objective is to quantify the impact that a service loss or asset would have on a business, and to determine the likelihood of a threat or vulnerability to actually occur. The result of the "Business impact and Risk Analysis" is the Risk Register, a prioritized list of risks which must be subsequently addressed. In this subprocess the KRIs and strategic responses are defined.

- ***Assessment of Required Risk Mitigation:***

  This sub-process objective is to determine where risk mitigation measures are required, and to identify risk owners who will be responsible for their implementation and ongoing maintenance.

- ***Risk Monitoring:***

  The risk monitoring objective is to monitor the progress of counter measure implementation, and to take corrective action when and where necessary.

Process activities, methods and techniques:

The process activities map directly to the M_o_R processes:

- Identify;
- Assess;
- Plan;
- Implement.

These activities are connected to the sub-processes in the following way:

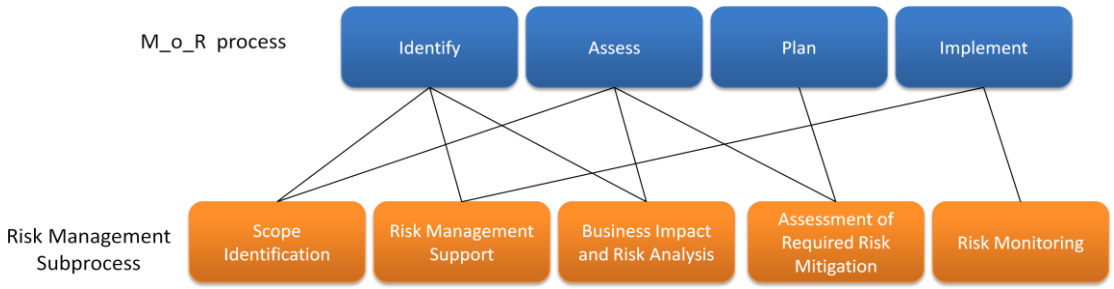

Fig. 18. M_o_R Process Mapped to Risk Management Sub-proceses.

- **Identify** and **Assess** on Strategy Risk Management (Scope Identification)
- **Identify** and **implement** on Risk Management Support;
- **Identify** and **Assess** on Business Impact and Risk Analysis;
- **Assess** and **Plan** Assessment of Required Risk Mitigation;
- **Implement** on Risk Monitoring;

Below we present a table relating activities with techniques and tasks to the risk management process:

Process Activities	Techniques	Tasks
Identify - Context	Stakeholder analysis. PESTLE analysis. SWOT analysis. Horizon scanning. Define the probability impact grid.	Examination of the activity information available.
Identify - Identify The Risks	Checklists. Prompt list. Cause and Effect diagrams. Group techniques (brainstorming, nominal group, Delphi). Questionnaries. Individual Interviews. Assumption Analysis. Constrains analysis. Risk descriptions.	Involve the most appropriate participants in the right manner, after having prepared them for their role. Identify the threats and opportunities, review, record the information on a risk register, structure the risk register, identify early warning indicators for KPIs.
Asses - Estimate	Probability assessment. Impact assessment. Proximity assessment. Expected value assessment.	Capture the probability of the identified threats and opportunities occurring and their impact (should they materialize), and also record the result in the risk register.
Assess - Evaluate	Summary risk profiles. Summary expected value assessment. Probability trees. Sensitivity analysis.	Capture the right information to allow the effective assessment of the relationships and interdependencies of the risks in their context. Build risk model.
Plan	Risk response planning. Cost-benefit analysis. Decision trees.	Address risks and maximize opportunities.
Implementation	Update summary risk profiles. Risk exposure trends. Update probabilistic risk models.	Executing, monitoring, controlling.

Table. 15. Risk Management Activities, Techniques and Tasks.

Triggers, inputs, outputs and interfaces:

Activities	Inputs	Outputs
Identify – Context	Regulatory framework and corporate governance requirements. Risk management policy. Risk management process guide. Activity documents. Lessons learned.	Activity analysis. Risk management strategy. Stakeholders map. Lessons learned.
Identify - Identify the risks	Activity analysis. Risk management strategy. Stakeholders map. Lessons learned. Issues.	Risk register. Early warning indicators.
Assess – Estimate	Risk register. Early warning indicators.	Risk register (agregation of risks and their impacts).
Assess – Evaluate	Risk register.	Summary risk profile. Relationship and interdependencies.
Plan	Summary risk profile. Relationships and interdependencies. Risk register. Existing insurance policies. Lessons learned.	Risk owner. Risk actionee. Risk register (including risk response and secondary risks). Risk response plan.
Implementation	Risk owner. Risk actionee. Risk register. Risk response plan.	Risk progress reports.

Table. 16. Risk Management Triggers, Inputs, Outputs and interfaces.

Key Performance Indicators:

- Annual review quality reports for management review;
- Quality reports for CAPA;
- Risk analysis updates;
- Risk analysis reviews;
- Product safety;
- Availability risk management team;
- Time until RMC is informed by CAPA or Safety Officer;
- Time until RMC is informed and there is a review risk analysis or informing PL;
- Duration of approval of records.

Information Management:

The Information Management is made through risk communication plan and risk progress report.

The **risk communication** plan describes how information will be disseminated to and received from all relevant stakeholders of a particular organization activity. A risk communication plan for that specific activity, or a specific risk communication plan, may be created.

The **risk progress** report is responsible for providing regular progress information to the management within a particular organization activity.

All documents must be connected as is explained in M_o_R framework and shown in the figure below.

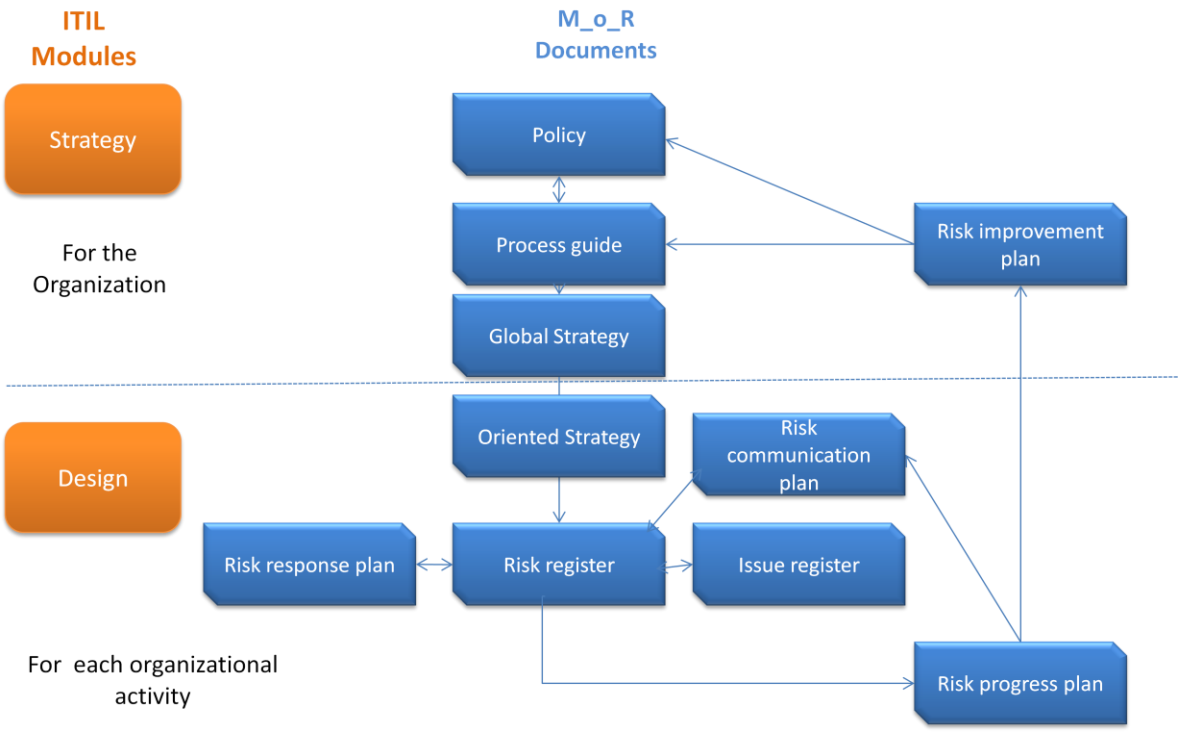

Fig. 19. Relationship Between Documents and ITIL Modules. Adapted from (38).

These documents will help clarify where other subsets of the organization may establish their own modified approach to meet the specific needs of its objectives, context and stakeholders.

The Set of all Risk documents to be used such as risk register, risk improvement plan and risk progress report are available in Management of Risk: Guidance for Practitioners(38)

Roles and Responsibilities:

Risk Manager - Process Owner:

The Risk Manager is responsible for identifying, assessing and controlling risks.

This includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats.

Bellow the responsibility matrix is showed.

ITIL Role | Sub-Process	Risk Manager	Other roles involved
Risk Management Support	A[1]R[2]	R
Business Impact and Risk Analysis	AR	
Assessment of Required Risk Mitigation	AR	
Risk Monitoring	AR	

[1] *A: Accountable* according to the RACI Model: Those who are ultimately accountable for the correct and thorough completion of the ITIL Business Relationship Management process.

[1] *R: Responsible* according to the RACI Model: Those who do the work to achieve a task within Business Relationship Management

Table. 17. Risk Management Responsibility Matrix.

All process members must be informed and consulted about risks.

Challenges, Critical Success Factors and Risks

The main challenges of Risk management are:

- To measure risks properly;
- To structure a good risk management transversally to all organization;
- To sensitize the organization to the importance of having a well-structured and documented risk management.

Potential Risk	Key Risk Indicator	Strategic Response
Commitment of the business to the Risk Management process.	Number of recognized risks. Risk Analysis Updates. Risk Analysis reviews.	Having a defined board-level sponsor that should be communicated to all staff.
A lack of senior management commitment or a lack of incentives for the participation in risk management.	Annual Review Quality Reports for Management Review.	Having risk responsibility clearly defined at board and senior management level. Having risk delivery linked to performance objectives and performance reviews. Communicating and emphasizing risk managment sucesses and improvements. Ensuring risk management functions has a direct reporting line to a senior executive.
Inability to recognize risk. Underestimate risk	Number of recognized risks.	Benchmarketing of risk management awareness. Regular reviews/questionaires to gauge risk managment awareness. Regular presentations on key risks and progress on the risk treatment plan to the internal audit committee.

Table. 18. Potential risks, KRIs and Strategic Response for Risk Management.

3.4. Service Transition

The objective of ITIL Service Transition is to build and deploy IT services. Service Transition also makes sure that changes to services and Service Management processes are carried out in a coordinated way while controlling the risks of failure and disruption. Associated to this model, there are some risks that have already been identified by ITIL(23), such as:

- Change in accountabilities, responsibilities and practices of existing projects that de-motivate the workforce;
- Alienation of some key support and operations staff;
- Additional unplanned costs to services in transition;
- Resistance to change and circumvention of the processes due to perceived bureaucracy;
- Excessive costs to the business caused by overly risk-averse Service Transition practices and plans;
- Knowledge sharing (as the wrong people may have access to information);
- Lack of maturity and integration of systems and tools resulting in people 'blaming' technology for other shortcomings;
- Poor integration between the processes - causing process isolation and a silo approach to delivering ITSM;
- Loss of productive hours, higher costs, loss of revenue or perhaps even business failure as a result of poor service transition processes.

In this section we will identify the process responsible for dealing with the identified main risk in ITIL and identify the KRIs and the strategic response to each one.

3.4.1. Evaluation

The Evaluation objective is to assess major changes, like the introduction of a new service or a substantial change to an existing one, before they are allowed to proceed to the next phase of their lifecycle. This Evaluation starts with risk identification and assessment(23). Following the M_o_R, the following sub-steps are mapped in Evaluation:

- **Identify and Plan** on Change Evaluation prior to Planning;
- **Assess** on Change Evaluation prior to Build;
- **Assess and Implement** on Change Evaluation prior to Deployment;
- **Assess and implement** on Change Evaluation after Deployment.

The Critical Success Factors to the Evaluation process are:

- Evaluate assertive changes;
- Determine if organization performance is acceptable;
- Identify the risk for being managed by Risk Management.

Potential Risk	Key Risk Indicator	Strategic Response
Developing standard performance measures and measurement methods across projects and suppliers.	Number of performance measures created. Number of performance measures documented.	Create the Change Evaluation Report. Change evaluations may be used at different points in a change's lifecycle, for example before authorizing the Change/Release build or during the Post Implementation Review.
Projects and suppliers inaccurately estimating delivery dates and causing delays in scheduling evaluation activities.	Time for Change Approval/ Rejection. Time evaluation.	Create a formal procedure to estimate milestones (delivery dates, goals). Establish accorded SLA for evaluation.
Not understanding the different stakeholders' perspectives that underpin effective risk management for the evaluation activities.	Documentation with risk management elements.	Agree on what risk management is for the organization. Use ISO31000 methodologies principles and concepts for Risk management (M_o_R is strongly recommended).
Not understanding nor being able to assess the balance between managing risk and taking risks as it affects the overall strategy of the organization and service delivery.	Numbers of risks taken in the organization. Impact of risks taken in the organization.	Take management risk strategic response (see risk management process). After making a decision, treat risk as soon as possible.
Not understand the impact of service transition services and releases.	Documentation with risk management elements. Number of risks taken in the organization. Impact of risks taken in the organization.	Building a thorough understanding of risks that have impacted or may impact successful service transition of services and releases. Communicating the organization's attitude to risk and effectively approach risk management during risk evaluation. Taking a pragmatic and measured approach to risk.
Deficit on sharing risk management information.	Documentation with risk management elements. Communication channels in organization.	Encouraging a risk management culture in which people share information. Create communication channels.
Introduction of major changes.	Number of new services.	Establish what is expected for service changes (downtown time, new features, working hours, outputs, and so on) early on. Establish priory tests.

Table. 19. Potential risks, KRIs and Strategic Response for Evaluation.

3.4.2. Service Asset and Configuration Management

The Service Asset and Configuration Management objective is to maintain the information about the configuration items required to deliver an IT service, including their relationships(23).

- **Identify** on Configuration Identification;
- **Assess and Plan** on Configuration Control;
- **Implement** on Configuration Verification and Audit.

The Critical Success Factors include:

- Focusing on establishing valid justification for collecting and maintaining data at the agreed level of detail;
- Demonstrating a top-down approach - focused on identifying service CIs and subsequently the CIs that support those services. Thereby allowing a rapid and clear demonstration of potential points of failure for any given service;
- Setting a justified level of accuracy, i.e. the correlation between the logical model within SACM and the “real world”;
- Making use of enabling technology to automate the CMS practices and enforce SACM policies.

Potential Risk	Key Risk Indicator	Strategic Response
Temptation to consider it technically focused, rather than service and business focused, since technical competence is essential to its successful delivery.	Staff skills.	Pay attention so as to not focus process just on technology but on staff skills too. To train the staff to deal with contingency plans and communication knowledge about configuration.
Degradation of the accuracy of configuration information over time.	Frequency of verification of CMS contents.	Have a routine configuration upgrade during which when a service is updated, its information is upgraded simulteanously too.
The CMS becomes out-of-date due to hardware assets being moved by non-authorized staff.	Frequency of verification of CMS contents. Number of unauthorized changes automatically detected. Number of incidents due to inaccurate CMS Information.	Have a set of authorized (owners) staff to services. Half-yearly physical audits should be conducted with discrepancies highlighted and investigated; managers should be informed of inconsistencies in their areas.
Lack of commitment and support from the management that do not understand the key role it must play supporting other processes.	Number of incidents due to inaccurate CMS Information.	Attracting and justifying funding for SACM through fundamented arguments and documentation.

Table. 20. Potential risks, KRIs and Strategic Response for SACM.

3.4.3. Release and Deployment Management

The Release and Deployment Management Objective aims to plan, schedule and control the movement of releases to test and live environments. The primary goal of Release Management is to ensure that the integrity of the live environment is protected and that the correct components are released(23).

- **Identify, Assess, Plan and Implement** on Release Management Support;
- **Plan** on Release Planning;
- **Assess and Plan** on Release Build;
- **Implement** on Release Deployment;
- **Implement** on Early Life Support;
- **Assess, Implement** on Release Closure.

The Critical Success Factors include:

- The new or changed service capability and resources are built in the target environment or deployment group;
- The new or changed service has been tested against the Service Design;
- The service capability has been proved in a pilot deployment;
- Re-usable test models are developed, which can be used for regression testing in future releases.

Potential Risk	Key risk Indicator	Strategic Response
Poorly defined scope and understanding of dependencies.	Number of releases. Duration of major deployments. Number of release backouts. Proportion of automatic release distribution.	Use strategy service documents to support releases and deploymens. Create a release planning, assigning authorized changes to release packages and defining the scope and content of releases. Based on this information, the release planning process develops a schedule for building, testing and deploying the release. Create a process responsible for deploying the release components into the live production environment. This process will be also be responsible for training end-users and operating staff, and circulating information/ documentation on the newly deployed release or the services it supports.
Using staff that is not dedicated to release and deployment activities, especially if the effort will take a significant amount of their time.	Amount of deployment hours. Amount of deployment effort.	Give ownership of release and deployment activities to a dedicated role. If the amount of time and efford of this activities exceeds staff working hours, then there must be charge to a specialized and dedicated staff.
Inadequate Management.	Staff skills.	Definition of leadership (responsible, role, deadlines, goals, practices). Definition and communication of corporate polices.
Lack of definition of the required controls, which leads to poorly evaluated and unauthorized changes, which adversely affect release and deployment plans. Unexpected changes in regulatory controls or licensing requirements.	Performance measurament requirements.	Developing standard performance measures and measurement methods across projects and suppliers.
Not being able to management organizational change.	Human soft skills. Expectations/objectives and roles documented.	Clearly define expectations/objectives and roles from customers, users, suppliers and other stakeholders using proper documentation and the organization‘s communication channel. Analyze the staff‘s soft skills with the RH department help. Always maintain available and easy to access information about releases, deployment procedures and encourage staff education.
Poor commitment and decision making. Indecision or late decision making. Failure to obtain appropriate approval at the right time.	Incidents due to decising making.	Do not commit beyond the organization‘s capacity. Support decision making on performance mesurament and experts experience.
Lack of operational support.	Risk responsabilites.	Inclusion of risk management responsibilites in job description and personal objectives.
Inadequate or inaccurate information.	Documentation. Rate of comunication channels use.	Maintain documentation updated. Maintain comuncation channels available and incentive stakeholders to use it.
Health and safety are compromised.	Work acidents. Staff skills.	Follow guidelines of helath and safety that protect the staff‘s well-being and security.

		Just allow trainned staff to upgrade and update organizations systems.
Inadequate 'back-out' or 'contingency' plan if sourcing/partnering fails.	Supported number of vital business components.	Mantain releases and backups. Do backups before starting updates and upgrades.
Application/technical infrastructure risks: Inadequate design. Professional negligence. Human error/incompetence. Differences/dependencies in infrastructure/applications. Increased dismantling/decommissioning costs. Safety being compromised. Performance failure (people or equipment). Breaches in physical security/information security.	Staff skills. Rate of communication channels used. Percentace of allocated staff/resources.	Maintain infrastructures as flexible as possible (use modules or tier modules). Document all structure architecture and design. Invest in training and comunication Previously plan staff, resources, and time allocation for updates and upgrades.

Table. 21. Potential risks, KRIs and Strategic Response for RDM.

3.4.4. Service Validation and Testing

The Service Validation and Testing process objective is to ensure that deployed releases and the resulting services meet customers' expectations and to verify that IT operations are able to support the new service.

The most frequent challenges to effective testing are due to a lack of respect and understanding of its role. Traditionally, testing has been in great need of funding(23).

- **Identify, Assess and Plan** on Test Model Definition;
- **Identify and Assess** Release on Component Acquisition;
- **Implement** on Release Test;
- **Assess and Implement** on Service Acceptance Testing.

The Critical Success Factors include*:*

- Understanding the different stakeholders' perspectives that underpin effective risk management for the change impact assessment and test activities;
- Building a thorough understanding of risks that have caused an impact or may impact successful Service Transition of services and releases;
- Encouraging a risk management culture where people share information and take a pragmatic and measured approach to risk;
- Quality is built into every stage of the service lifecycle using a structured framework, such as the V-model;
- Issues are identified early in the service lifecycle;
- Testing provides evidence that the service assets and configurations have been built and correctly implemented, in addition to the service delivering what the customer needs;
- Re-usable test models are developed, which can be used for regression testing in future releases.

Potential Risk	Key Risk Indicator	Strategic Response
Unclear expectations/objectives.	Number of objectives/goals. Number of tests. Number of stakeholders. Number of identified risks.	Define Service goals. Define what must be tested and validate it with stakeholders. Understand the different stakeholder***s***‘ perspectives that underpin effective risk management for the change impact assessment and test activities. Build a thorough understanding of risks that have made an impact or may impact successful service transition of services and releases. Issues are identified early in the service lifecycle.
Inability to maintain test environment and test data that matches the live environment.	Number of variables tested. Number of errors detected in the live environment that were not detected in the test environment	End users and the usual environment of output of the service should be used for testing.
Lack of understanding of the risks means that testing is not targeted at the critical elements that need to be well-controlled and therefore tested.	Number of problems detected in critical elements Number of tests targeting critical elements.	Understanding the different stakeholder***s***‘ perspectives that underpin effective risk management for the change impact assessment and test activities. Building a thorough understanding of risks that have made an impact or may impact successful service transition of services and releases. Issues are identified early in the service lifecycle.
Resource shortages (e.g. users, support staff, and so on) introduce delays and have an impact on other service transitions.	Time of test. Time of validation. Resources number.	Have SLAS defined for testing and validation. Estimate resources (skills, time, staff, and so on) needed, according to tests/validations to be done. Re-usable test models are developed, which can be used for regression testing in future releases.
Projects and suppliers inaccurately estimate delivery dates, causing delays in scheduling Service Transition activities.		

Table. 22. Potential risks, KRIs and Strategic Response for Service Validation and Testing.

3.4.5. Knowledge Management

Knowledge Management's objective is to gather, analyze, store and share knowledge and information within an organization. The primary purpose of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge. ITIL Knowledge Management is dealt with in many other Service Management processes. The Knowledge Management process itself ensures that all the information used within Service Management, and stored in the Service Knowledge Management System, is consistent and readily available(23).

The Critical Success Factors are:

- Gather knowledge;
- Maintain organization up-to-date.

Potential risks, KRIs and strategy responses are:

Potential Risk	Key Risk indicator	Strategic Response
Inability to gather pertinent knowledge for organization.	Documentation. Frequency of training. Frequency of knowledge updates.	Create a Service Knowledge Management System (SKMS). SKMS is a central repository of the data, information and knowledge that the IT organization needs to manage the lifecycle of its services. Its purpose is to store, analyze and present the service provider's data, information and knowledge. The SKMS is not necessarily a single system - in most cases it will be a federated system based on a variety of data sources.

Table. 23. Potential risks, KRIs and Strategic Response for Knowledge Management.

3.5. Service Operation

The objective of ITIL Service Operation is to make sure that IT services are delivered effectively and efficiently. This includes fulfilling user requests, resolving service failures, and fixing problems as well as carrying out routine operational tasks. The risk management on this module is around organization routine and focuses on delivering and supporting all services at the same time. So part of risk management on this module is to monitor services, identify risks and make sure they do not materialize. Operation managers should work closely with Service Design and Service Transition to provide the operation perspective, thus ensuring that design and transition outcomes support the overall operational needs.

3.5.1. Event Management

The Event Management process objective is to make sure CIs and services are constantly monitored and to filter and categorize events in order to decide what the appropriate actions are(24).

The M_o_R mapping for the sub-processes is:

- **Identification, Assess, Plan and Implementation** on Maintenance of Event Monitoring Mechanisms and Rules;
- **Plan and Implement** on Event Filtering and 1st Level Correlation;
- **Implement** on 2nd Level Correlation and Response Selection;

- **Implement** on Event Review and Closure.

The most important Critical Success Factor is achieving the correct filtering level. There are three keys to the correct level of filtering, as follows:

- Integrate event management into all service management processes where feasible, which will ensure that only the events significant to these processes are reported;
- Design new services with event management in mind;
- Trial and error. No matter how thoroughly event management is planned, there will be classes of events that are not properly filtered. Event management must therefore include a formal process to evaluate the effectiveness of filtering.

Potential risks, KRIs and strategy responses are:

Potential Risk	Key Risk Indicator	Strategic Response
Determine a wrong level of Filtering.	Number of filters.	Create event filtering and correlation rules that determine if an event is significant and to decide upon an appropriate response. Some of those rules must be defined during the service design stage, for example to ensure that events are triggered when the required service availability is endangered.
Failure to maintain momentum in rolling out the necessary monitoring agents across the IT Infrastructure.	Events categorized.	Categorize and catalog events. Mantain an event record.

Table. 24. Potential risks, KRIs and Strategic Response for Event Management.

3.5.2. Incident Management

The Incident Management process objective is to manage the lifecycle of all incidents. The primary goal of Incident Management is to return the IT service to users as quickly as possible(24).

The M_o_R process map is:

- **Identify, Assess, Plan and Implement** on Incident Management Support;
- **Implement** on Incident Logging and Categorization;
- **Implement** on Immediate Incident Resolution by 1st Level Support;
- **Implement** on Incident Resolution by 2nd Level Support;
- **Implement** on Handling of Major Incidents;
- **Implement** on Incident Monitoring and Escalation;
- **Implement** on Incident Closure and Evaluation;
- **Implement** on Pro-Active User Information;
- **Implement** on Incident Management Reporting.

The main CSF for the Incident Management process are:

- Establish a good Service Desk is key to a successful Incident Management;
- Clearly defined targets to work to - as defined in SLAs;

- Adequate customer-oriented and technically trained support staff that should have the correct skill level at all stages of the process;
- Integrated support tools to drive and control the process.

The risks to successful Incident Management are actually similar to some of the challenges and the reverse of a few of the CSFs mentioned above. Below we specify the KRIs for each one and the respective strategic response.

The potential risks, KRIs and strategy responses are:

Potential Risk	Key Risk Indicator	Strategic Response
Overflow of incidents that cannot be handled within acceptable timescales due to a lack of available or properly trained resources.	Number of incidents. Number of repeated incidents. Incident resolution time. Incidents remotely solved.	Try to detect incidents as early as possible. This will require users reporting incidents to be educated, the use of Super Users and the configuration of event management tools. Availability of information about problems and known errors, which will enable incicent management staff to learn from previous incidents and track the resolutions‘ status.
Resolution of is being delayed and not developed as intended because of inadequate support tools to raise alerts and prompt progress.	Incidents remotely solved. Average initial response time. Incident resolution time. Resolution within SLA. Incident resolution effort.	Use of ITSM tools such as Easyvista, Hp Service Desk or Remedy. Convincing all staff (technical teams as well as users) that all incidents must be logged, and encourage the use of self-help web-based capabilities (which can speed up assistance and reduce resource requirements).
Mismatch in objectives or actions owing to poorly aligned or non-existent OLAs and/or UCs.	Definition of OLAs.	Integration into the SLM process. This will help incident management to correctly assess the impact and priority of incidents as well as assist in defining and executing escalation procedures. SLM will also benefit from the information learned during incident management like for example in determining whether service level performance targets are realistic and achievable.
Lack of adequate and/or timely information sources because of inadequate tools or lack of integration.	Number of incident escalations.	Integration into the CMS to determine relationships between CIs and refer to the history of CIs when performing first-line support.

Table. 25. Potential risks, KRIs and Strategic Response for Incident Management.

3.5.3. Request Fulfillment

The request fulfillment objective is to deal with service requests from the users which in most cases are minor changes or requests for information(24).

Request fulfillment depends on the following Critical Success Factors:

- Clearly define and document the type of requests that will be handled within the request fulfillment process (and those that will either go through service desk and be handled as incidents or those that will need to go through formal change management) - so that all parties are absolutely clear on that scope.

- Establish self-help front-end capabilities that allow users to interface successfully with the request fulfillment process.

The potential risks, KRIs and strategy responses are:

Potential Risk	Key Risk Indicator	Strategic Response
Poorly defined scope, which means people are unclear about what exactly the process is expected to handle with.	Number of requests.	Definition and document of scope and goal. Create a request model defining specific agreed steps that will be followed for the service request. Create a record request containing all details of the service request.
Poorly designed or implemented user interfaces so that users have difficulty raising the requests they need.	Number of requests.	Create a request model defining specific agreed steps that will be followed for the service request.
Badly designed or operated back-end fulfillment processes that are incapable of dealing with the volume or nature of the requests being made.	Number of requests.	Definition and documentation of scope and goal. Create a request model which defines specific agreed steps to be followed for the service request.
Inadequate monitoring capabilities so that accurate metrics cannot be gathered.	Metrics gathered.	Create a service request status information containing the present status of the service request sent to a user, who earlier reported a service. Status information is typically provided to users at various points during a service request's lifecycle.

Table. 26. Potential risks, KRIs and Strategic Response for Request Fulfillment.

3.5.4. Problem Management

The problem management process objective is to manage the lifecycle of all problems. The primary objectives of Problem Management are to prevent incidents from happening, and to minimize the impact of incidents that cannot be prevented. Proactive Problem Management analyzes Incident Records, and uses data collected by other IT Service Management processes to identify trends or significant problems(24).

A major dependency of Problem Management in risk management is the establishment of an effective Incident Management process and tools. This will ensure that problems are identified as soon as possible and that as much work is done on pre-qualification as possible. However, it is also critical that the two processes have formal interfaces and common working practices. This implies the following:

- Linking Incident and Problem Management tools;
- The ability to relate Incident and Problem Records;
- The second- and third-line staff should have a good working relationship with the staff on the first line;
- Making sure that business impact is well-understood by all staff working on problem resolution.

In addition, it is important that Problem Management is able to use all Knowledge and Configuration Management resources available.

Another Critical Success Factor is the ongoing training of technical staff in both technical aspects of their job as well as the business implications of the services they support and the processes they use.

Potential risks, KRIs and strategy responses are:

Potential Risk	Key Risk Indicator	Strategy Response
Occurrence of recurrent problems.	Number of problems. Problem resolution time. Number of unresolved problems. Time until problem identification. Problem resolution effort.	Try to identify the source of the problem. Identify why problem is not resolved. Assess the impact of this recurrence in the organization. Have staff specialized on tests and quality.
Inability to use previous knowledge to resolve problems.	Number of problems. Number of unresolved problems.	Motivate staff to use the knowledge database.
Incident management and problem management are disconnected.	Number of incidents per known problem.	To have a continual communication channel between the incident management group and the problem management group.

Table. 27. Potential risks, KRIs and Strategic Response for Problem Management.

3.5.5. Access Management

The Access management goal is to grant authorized users the right to use a service while simultaneously preventing access to non-authorized users. The Access Management processes essentially execute policies defined in Information Security Management. Access Management is sometimes also referred to as Rights Management or Identity Management(24).

The CSFs for Access Management are:

- The ability to verify the identity of the stakeholders;
- The ability to manage changes to a user's access requirements.

Potential risks, KRIs and strategy responses are:

Potential Risk	Key Risk indicator	Strategy Response
Unnable to restrict access rights to unauthorized users.	Number of access. Number of authorized access. Number of unauthorized access.	Always keep users database updated. Keep a flexible system linked to the ability to manage changes to a user's access requirements, and give multiples access rights according the roles in the organization.
System is difficult to access.	Number of access.	Keep a flexible system accessible.
Inability to track users' access.	Number of access.	Use specialized tools.

Table. 28. Potential risks, KRIs and Strategic Response for Access Management.

3.6. Continual Service Improvement

The Continual Service Improvement (CSI) process uses methods from quality management in order to learn from past successes and failures. The CSI process aims to continually improve the effectiveness and efficiency of IT processes and services in line with the concept of continual improvement adopted in ISO 20000. For this it is vital to integrate risk management into the culture of the organization, and to explain how this can be achieved and highlight the need for regular review.

While Risk Management in design and transition stages must organize concepts and mainly identify risks of the service *lifecycle*, a good CSI *program* will assess the results of Risk Management *a*ctivities to identify service improvements. This can be done through risk mitigation, elimination and management as well as by regularly reviewing the goals to be achieved in order to ensure risk management is being appropriately and successfully handled across the organization. For this it is important to embed risk management into the organization's culture and put mechanisms in place to review and confirm that the approach to risk management remains appropriate given the organization's objectives and context. Following we present the steps of a successful CSI wrapping:

- Embedding and reviewing M_o_R Step;
- Embedding the M_o_R principles into the organization;
- Changing the culture for risk management;
- Measuring the value through a Service Measurement process;
- Overcoming the common barrier to success;
- Identifying and establishing opportunities for change.

To achieve this it is important to have a closed-loop feedback system based on the Plan-do-check-act (PDCA) model specified in ISO/IEC 2000, which is established and capable of receiving inputs for change from any planning perspective.

3.6.1. 7 Steps Improvement Service

Fundamental to CSI is the concept of measurement. CSI uses the 7-Step Improvement Process that consists in:

1. Define what you should measure;
2. Define what you can measure;
3. Gathering the data;
4. Processing the data where data is processed in alignment with the specified CSFs, KPIs and KRI's;
5. Analyzing the data and finding the strategic response;
6. Presenting and using the information;
7. Implementing corrective action.

While these seven steps of measurement appear to form a circular set of activities, in fact, they constitute a knowledge spiral. In practice, the knowledge gathered and wisdom derived from that knowledge (at one level of the organization) becomes a data input to the next(25).

So the CSF are:

- To encourage the organization to continuously improve services;
- Measure information with meaning for the organization.

Potential risks, KRIs and strategy responses are:

Potential risk	Key risk indicator	Strategic Response
Services became static throughout time.	Service evolution. Percentage of new services.	Implement the seven steps improvement process, according to the organization.
Inability to identify elements to measure.	Number of elements to be measured.	In the first step, plan what information must be gathered and decide what will be done with it. Still in first step the customer and the organization must sit together to discuss what should be measured or to identify the purpose of the data gathered in the first place. Do not try to measure everything.

Table. 29. Potential risks, KRIs and Strategic Response for 7 Steps Improvement Service.

3.6.2. Service Reporting

The objective of this process is to create business historical representation of the past period's performance that portrays organization experience(25).

The CSFs are:

- Reports focusing on the future as strong, based on organization history;
- Right content for the right audience.

Potential risk	Key risk indicator	Strategic Response
Inability to keep continous reporting.	Percentage of organization goals tracked.	Simple, effective, customizable and automated reporting.
Inability to provide the right content for the right audience	Access to reports and the medium to be used.	Keep a report framework that maintains the previous types of reporting, according to the stakeholder Targeted audience(s) and the related business views on what the service delivered is. Reports must be unambiguous and have relevant information in a language and style stakeholders understand and like. It should be accessible in the medium of their choice, and detail the delivery of IT into their environment within their boundaries, without such information being clouded by the data related to the delivery of IT into other areas of the business. Be careful about the type of charts and graphs used. They must be understandable and not opened to different interpretations.
Inability to keep reporting update.	Number of updating. Number of report schedules.	Agreement on what to measure and what to report on agreed definitions of all terms and boundaries. Meetings scheduled to review and discuss reports. Basis of all calculations.

Table. 30. Potential risks, KRIs and Strategic Response for Service Reporting.

3.6.3. Service Measurement

This process is responsible for measuring services according to three basic measurements that most organizations use: Availability, Reliability, and Performance. These measurements are connected to design services and its processes. Therefore, some of design services KRIs could be applied to this process(25).

The CSF are:

- Creation of a Service Measurement Framework;
- Create Smart Performance Targets.

Potential risks, KRIs and strategy responses are:

Potential risk	Key risk indicator	Strategic Response
Identify measurement useless.	Number of metrics.	Different levels of measurement and reporting.
Not identify the right filtering in measure.	Number of metrics.	Service measurement is not about assigning blame or protecting oneself but about providing a meaningful view of the IT service as the customer experiences the service. Always have in mind that the measurement purpose is to achieve organization improvement. Go further than the component level.

Table. 31. Potential risks, KRIs and Strategic Response for Service Measurement.

4. Demonstration

This case study is an extension of Disney's ITIL® Journey paper (39), which was based on Disney's ITIL. Our intention is to provide an example of a theoretical implementation of this model in a big organization.

4.1. Case Study

First of all it's important to define a team to take charge of risk management of IT services. This team must be composed by staff with ITIL and risk management qualifications. In case of Disney it was necessary to give formation in ITIL foundation to the employees so for Risk management team it's important to give risk management formation too (at least until our risk model is not completed incorporated in ITIL practices).

Risk in big organizations (ideally) is defined in layers and is done by a specialized team, the same happened for Disney. Risk Management in ITIL, as in all ITIL Implementations, is started by aligning IT with the business and the organization's goals in the strategy module. Part of this entails defining the risks that the organization is willing to accept or not. So the first step is entailing marketing ITIL and risk management process from executive level down, and spread all information about organization risk boundaries. For Disney, for instance, bad publicity, bad installations and technology are risks that can kill business, but there are thousands of other risks that may not be relevant as a threat or not be worthy of taking into consideration because of their impact or probability (for example, a bee attack at one of the parks, or a kid losing a teeth in the parks). In ITIL process, it is important for all the service strategy owners to work together to decide with the risk manager what must be taken into consideration and what is not in order to define the limits of the organization. Some of Disney's high levels CFS are (40) :

- Leading diversified international family entertainment and media enterprise;
- Be the most respected and beloved brands around the globe;
- Generating the best creative content possible, fostering innovation and using the latest technology;
- 100% availability, reliability and maintainability.

These CSFs immediately remind us of some potential risks that are crucial threats to the business, such as:

- Technological problems;
- Safety and security problems;
- Logistic problems
- Media problems (bad publicity, communication misunderstandings) ;
- ensure that widespread change does not result in incidents
- Lack of innovation and leadership;
- …

Of course this is just the first level of CSF and potential risks.

For each CSF/potential risk a response must be planned, must be linked to a department/responsible/service and each Disney segment must be aware about the high level CSFs and have an assigned owner for them and for threat them according to the risk management owner's planning.

In the following Design Process, when all services have been defined to all Disneys' 5 segments the micro CFS must be determined. The ideal is to define the top CSFs and spread them to the organization's lower levels. It is important not to drag this over time. In the beginning of the process a time schedule to define risk management limits must be imposed.

After the strategy has been defined as well as risk management limits, the first CSF and Potential risks have to be defined, oganizations must design the services.Sequence of Design services /risk management inputs are pictured in figure 17.

According to our Model the service design level starts with the **business impact and risk analysis** sub-process at which point the likelihood of a threat or vulnerability of risk is defined as well as KRIs, according to the CSFs. This phase is typically made by the direct responsible for the parks and by the organization's physical structures. They create specific CSFs for each physical organization unit and services, and inform managers about starting the definition of potential risks and KRIs with them. In this phase all knowledge about risk is diffused. In the case of The Walt Disney Company (TWDC), the process of defining potential risk must be done by parts, from operation to strategy business modules. The operation staff is organized to define potential risks and the respective KRIs, and as a list of potential risk is being created, the level of potential risk is being redefined until we achieve CSF for the organization at the operational level.

Some of the vital requisites for TWDC's IT sources, for instance, are 100% availability, reliability and maintainability. It means that we have to ensure that widespread change does not result in incidents. In other words, we need to define potential risks and KRIs so that we are sure-footed and confident about our release management and new capabilities.

Besides the potential risks and KRIs described in Chapter 6 for access management, some specific ones are for instance: After employee left organization proceed to cancel all his access rights in the organization, Employees only have access to information vital to their work, etc.

Potential Risk	Key Risk indicator
Employee continue having access to systems after they left TDWC.	Number of unauthorized access.
Employees have access to information that is not related to their work	Number of unauthorized access
Trade of access credentials among employees	Number of access from different locations to the system

Table. 32. Potential risks, KRIs for Access Management for Disney's Case

After the creation of knowledge about risk in the organization's assessment of required risk, mitigation is put into action to determine where **risk mitigation** measures are required, and to identify Risk Owners who will be responsible for their implementation and ongoing maintenance.

As a result, the process in how the M_o_R Steps will be implemented amid ITIL process must be defined.

In addition, an organization is supposed to have a **continuous support** that defines a framework for risk management that continually identifies risk across the organization, and, most importantly, this process specifies how risk is quantified, what risks the organization is willing to accept, and who is in charge of the various Risk Management duties.

5. Evaluation

In this section we present our evaluation process, the data collected during our evaluation stage and finish by presenting our conclusions about the collected data.

5.1. Evaluation process

- 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.

For the interview process we chose half an hour semi-structured interviews, having the following questions as guidelines:

1. In your opinion, does the present ITIL version provide effective mechanisms for risk management?
2. When implementing ITIL in an organization, how do you implement risk management?
3. Do you think that a new risk management process would improve the implementation of ITIL in organizations? Why?
4. Do you think the addition of KRI's to ITIL brings an added value to ITIL?
5. What advantages do you see from implementing our model?
6. What disadvantages do you see from implementing our model?
7. What do you think about our proposed model in general?

5.2. Evaluation Results

5.2.1. Feedback from Centeris[1] about Risk Management Model in ITIL article (37)

According to the reviewers, this paper provides an interesting approach to map the ITIL process, according to the M_o_R processes, and ensures a better risk management implementation so they supported its publication.

5.2.2. Feedback from Social Networks

My opinion is that in ITIL we mainly categorize and prioritize the CI or IT Service by using 'Vital Business Function (VBF)'. This way we could cover the risk management through BCP and DRP to some extent.

Senior Consultant, IT Consultant, Brazil

It may not be ONE of these 27 'things', but it's definitely there (risk management process): there's plenty of Risk Management in ITIL, but you have to recognize it, that is the problem. Risk Management is actually a very peculiar process: it is not triggered by other tactical or operational IT management processes. The only connection is through data, which gives Risk Management a completely different profile from the essentially reactive Problem Management that was presented by ITIL - which actually was "Incident Management for high-impact-incidents".

There are the risks that you need to think about when you are doing Service Design, there it is embedded somewhere around Availability and IT Service Continuity, as one would expect. So a clarification on identify risks, analyze cause, determine countermeasure, take action and evaluate is welcomed.

Senior Consultant, IT Consultant, Brazil

Microsoft has created the Risk Management Discipline in their Microsoft Operations Framework. At first it was set apart from the other functions and in their recent released version 4 it is part of the function Governance, Risk and Compliance. When you zoom in on Risk Management you'll find an overlap with other functions/processes, specifically problem management. When you talk about proactive problem management, you'll come into the realm of risk management. Specifically when discussing possible scenarios (what can go wrong and how can we prevent this from happening?)

In the Operations Management course I've given last week, I've spend a good couple of hours on risk management. Every time I'm surprised to find that most system administrators (the course is meant for operations managers, team leaders and technical supervisors) have difficulty identifying risks in production. They can easily identify project management risks (or risks for change management), but not risks in the day-to-day running of IT services. And according to Forrester and others (I do not have the survey reports ready, so I'm now prime target for the craptoid facts) about 80% of downtime is caused by changes that are implemented hastily and untested and by

[1] http://centeris.eiswatch.org/

administrators not following procedures or just being sloppy. I feel that spending some time on identifying risks and coming up with ways to mitigate them will be very useful. Also, are workarounds for incidents not some kind of contingency plans in the Risk management sense?

5.2.3. Feedback from face-to-face interviews with experts

Luís de Matos Senior Consultant at Easyvista, Portugal

"There are many viewpoints to risks.

There are the risks that you need to think about when you are doing Service Design, there it is embedded somewhere around Availability and IT Service Continuity, as one would expect.

Also, one should not forget about the risks for the business, which I find are described in a quite interesting way in Service Strategy. We, IT people, certainly understand that whenever you start contemplating the possibility of using IT in some way, you are always in great danger. So this new model can be a great help to deal with risk."

Marcos Santos IT Project Manager at Ciplan, Brazil

"The new process is a good idea. That way there would not be the same problem that we have with security or quality. It is not MY task to think about them, it is the people who are managing it. So it is a good idea to have some condensed guidance for that."

Júlio Moreno Senior Project Manager at HP Enterprise Services, Portugal

"I see risk management in ITIL mostly in change management but when I need to manage risk at organizations, I use a parallel framework to construct a robust risk management. The proposal of this new model with the introduction of a new process and new metrics is valid and I think they could help avoid the use of extra frameworks".

João Caldeira Principal software Consultant and ITIL Expert at BMC Software, Portugal

"Today in all the projects that we implement risk management, we use an ad hoc approach. Because sometimes due to time constraints everything is urgent, there is no time to use a deeply conceptual approach. I think that the new risk management process in ITIL would bring an added value but in my opinion this process should be included in the service strategy because it is in this phase that organization framework and goals are defined."

Rui Gomes Informatics Administrator at HFF (Hospital Amadora-Sintra), Portugal

"Here we manage very delicate information: medical information. So the following of standards is very important. For risk management we follow the ISO270005 standard that is about risk management in IT. For us, and we are trying to for a long time, it would be important to implement a framework of best practices for service management like ITIL, but sometimes it is difficult to convince the board of the usefulness of spending money in a framework (ITIL can be expensive to implement).

One thing that would help us is if risk management was clarified in ITIL. This would elevate ITIL to COBIT's conditions."

Rogério Costa Certificated in ITIL V3 and Consultant at ITSMF and IT Manager at IIMF, Portugal

"There are some gaps and contradictions in ITIL Risk Management. When I need risk management guidelines (and because I use a lot of Microsoft technology), I take them from MOF. This new model would surely be an adding of value. But as a disadvantage of its implementation I see the identification of all KRIs as a complex and time/cost-consuming process."

5.3. Discussion

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 organization's aspects.

5.3.1. New Risk Management Process

Although it was supported by the majority of the interviewed consultants, the need for a new process for risk management is not consensual. However, all the interviewed experts provided a different definition for what risk management is nowadays. Clearly ITIL does not provide the consultants with a clear concept about how to treat risk. What was consensual among the experts was the necessity of a clarification in ITIL about how to implement risk management. Experts admit that risk management in ITIL is not satisfying. Some of them admit that they do risk management ad doc or parallel to ITIL, using other frameworks to do it.

For those who supported the new risk management process, its place was not consensual. Some of the experts defended that the place of the new process should be on the strategy module, others said that this process belongs just to the design module.

5.3.2. M_o_R steps amid ITIL Process

The clarification of risk management on ITIL processes was well accepted by all experts. Some of them argued that there are some risk management elements in ITIL already. However, they admitted difficulty in identifying an effective way to use them.

5.3.3. Introduction of KRI's

The introduction of new metrics in ITIL was also well accepted by all experts. The importance given to this element varied significantly and only one expert pointed out as an advantage the implementation of KRIs in the levels.

5.3.4. Advantages of the new model

The most frequently pointed out advantages to the use of this model were:

- Having the responsibility for risk management clearly assigned;
- Having consistent guidelines for the implementation of risk management among ITIL.

5.3.5. Disadvantages of the new model

The most frequently pointed out disadvantages to the use of this model were:

- Increased bureaucracy;
- Potential to an increase in costs and/or time (given that sometimes managing risk can be more expensive that the risk itself).

6. Conclusion

Risk management is essential to all organizations. The need of predicting and turning organizations prepared to face the unexpected with flexibility and agility is real in today's business environment. 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 and integrate it in the organization's services. Thus, the congregation of business modules, such as risk management and ITSM, is desirable.

The value of ITIL is undeniable as it helps reducing IT costs, increase IT performance and, at the same time, improve business performance through IT-business alignment. These qualities are vital for any organization.

In our literature review we exposed ITIL and the deficit of risk management guidelines in ITIL. In ITIL there is the definition of risk management. However, even nowadays with the recent update of ITILv3 in 2011, risk management implementation and risk response are vague. In fact, nothing about risk was updated in this new ITILv3 version, so it is difficult to have a strong risk culture by just using ITIL for IT service management in an organization. The information in the ITIL Library is still generalist and unsatisfactory. Compared to other IT service management frameworks, ITIL is weak in the risk management field. Consequently, how can organizations adopt a strong risk management in ITIL without neither changing the framework nor using externals mechanisms for risk management?

We think that to answer this question, it would be important to:

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

In our model, we tried to clarify the risk management embedding in this framework and reinforce it. To accomplish this we clarified and adjusted the place of M_o_R in this framework, mapping M_o_R process in ITIL sub-processes and adding two important concepts:

- KRIs;
- A new process response for risk management on Divided in the Strategy and Design Module.

These additional concepts provide an important help for the board and the stakeholders in dealing with risk in organizations, because it provides a guideline about how risk management must work in organizations, specifies metrics to identify risk management elements and links strategic responses to them.

In this work we define the recommendation in ITIL for KRIs and outlined only one or two KRIs per CFS. This document is not inclusive of all KRIs but simply an example of how KRIs may be mapped to processes. Additional KRIs can be added, according to the specific needs of each organization, always having in mind that based on what is important to the business and IT management, the KRIs may change over a period of time.

To evaluate this work we relied on experts' opinion about the proposed model and a case study.

The evaluation shows that project managers identify risk management in ITIL differently. There is no consensus about risk management process as ITIL. However, all experts state that new risk management elements in ITIL are needed and that our proposal would be an added value for ITIL. The Disney case study shows that a well-organized methodology, based on a solid structure, can be vital for a big company to achieve its goals and take a noticeable position in the business environment.

A continuation of this work would be a standardization of the ITIL process with a specific part of each process devoted to risk management guidelines instead of just some concepts of risk with a generic definition of what risk is.

To conclude on KRIs, another aspect that would be interesting to develop after this work is the defining of the Metrics required, Measurements, Responsibilities and Categories, and so on, as is already defined for KPIs in ITIL.

In this model we presented a set of artificially created guidelines according to the organization environment and experts' experience. Our work in the management of risk alongside ITIL can always be discussed and continued, providing a foundation for future work in the field.

References

1. *Methodologies of Support to the Execution of Risk Management.* **Nascimento, Luís, et al.** San Juan, PR : s.n., 2010. ICSTE 2010 - 2nd International Conference on Software Technology and Engineering. Vol. I, pp. 176-180.

2. **Crouhy, Michel, Galai, Dan and Mark.** *The Essentials of Risk Management.* s.l. : McGraw-Hill, 2005. 0071429662.

3. **Kouns, Jake, Minoli and Daniel.** *Information Technology Risk Management In Enterprise Environments.* Canada : Willey, 2010. 0471762547.

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

5. **Office of Government Commerce.** [Online] [Cited: December 01, 2010.] www.ogc.gov.uk.

6. **OGC - Office of Government Commerce.** *Managment of Risk Pocketbook - M_o_R OGC.* London : TSO, 2007. 9780113310760.

7. **Office of Government Commerce.** *ITIL.org - ITIL.* [Online] [Cited: December 10, 2010.] http://www.itil.org.

8. **Soares, Rui.** *ITIL Foundation in IT Service Management.* Portugal : GFI Portugal, 2009. Whitepaper.

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

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

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

12. **Vaishnavi, V. and Kuechler, W.** Design Research in Information Systems. [Online] January 20, 2004. [Cited: July 01, 2010.] http://desrist.org/design-research-in-information-systems.

13. **Hevner, Alan R., et al.** Design Science in Information Systems Research. University of Minnesota : MIS Quarterly, 2004, pp. 75-105.

14. *A Design Science Research Methodology.* **Peffers, Ken, et al., et al.** Volume 24 Issue 3 pp. 45-78. : s.n., Winter 2007-8.

15. *A process model for integrated IT governance, risk, and compliance management.* **Raz, Nicolas, Weippl, Edgar and Seufert.** s.l. : Palgrave Macmillan Journals, 2010, Vol. 7, pp. 155-170.

16. **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.

17. *Use and benefits of tools for project risk management.* **T. Raz, and Michael E.** 2001. International Journal of Project Management. Vol. 19, pp. 9-17.

18. *Developing Key Risk Indicators to Streangthen Enterprise Risk Management.* **Beasley, Mark S., Brauson, Bruce C. and Hancock, Bounnie V.** Thought Leadership in ERM, s.l. : COSO, December 2010.

19. **Office of Government Commerce.** M_o_R - Management of Risk. *M_o_R Official Site.* [Online] [Cited: December 01, 2010.] http://www.mor-officialsite.com/.

20. **Williams, Graham.** *Everything you wanted to know about Management of Risk: Guidance for Practitioners (M_o_R®) in less than one thousand words.* GSW Consultancy. 2009. Whitepaper.

21. **Office of Government Commerce.** *ITIL - Service Strategy.* London : OGC, 2007.

22. —. *ITIL – Service Design.* London : TSO, 2007.

23. —. *ITIL - Service Transition.* London : OGC, 2007.

24. —. *ITIL - Service Operation.* London : OGC, 2007.

25. —. *ITIL - Continual Service Improvement.* London : OGC, 2007.

26. **Valerie, Arraj.** *ITIL®: The Basics.* The APM Group. s.l. : Compliance Process Partners, 2010. Whitepaper.

27. **Pantaleão, Juliana.** *Lean process modeling on ITIL Services in EPF.* Instituto Superior Técnico (IST). 2009. MSc Thesis.

28. **Jesus, Gonçalo João Vitorino de.** *ITIL: Valerá a pena? Quais os processos mais afectados?* Coimbra : s.n., 2006.

29. *The Value of ITIL.* **Oliveira, Pedro C. B.** lisbon : s.n., 2009.

30. *Lessons Learned in ITIL Implementation Failure.* **Sharifi, Mohammad, et al.** Kuala Lumpur, Malaysia : IEEE, 2008. Information Technology, 2008. ITSim 2008. International Symposium on. pp. 1-4. 978-1-4244-2328-6.

31. **ISO 20000, ITIL.** [Online] [Cited: December 22, 2010.] http://20000.fwtk.org/iso-20000.htm.

32. **Faber, Michael and Faber, Rubina.** *ITIL® and Corporate Risk Alignment Guide An introduction to corporate risk and ITIL, and how ITIL supports and is assisted by Management of Risk (M_o_R®).* The Stationery Office (TSO). London : The Stationery Office, 2010. Whitepaper.

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

34. **T., Feglar.** ITIL based Service Level Management if SLAs Cover Security. Czech Republic : CITSA, 2004, pp. 61-71.

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

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

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

38. **Office of Government Commerce.** *Management of risk: Guidance for Practitioners.* Stationery Office 2010. 3rd. United Kingdom : TSO, 2010.

39. *Disney's ITIL® Journey.* **Taylor, Glen.** London : The APM Group and The Stationery Office, 2010.

40. Company Overview . *The Walt Disney Company.* [Online] 04 28, 2012. http://thewaltdisneycompany.com.

41. *Risk Management Model in ITIL.* **Vilarinho, Sarah, Silva and M, Miguel.** Portugal : s.n., 2011.

A. Publications

Vilarinho, Sarah; Silva, Miguel M. Risk Management Model with ITIL, CENTERIS, Sprinte 2011.

Vilarinho, Sarah; Silva, Miguel M. Risk Management Model in ITIL, Communications in Computer and Information Science, Vol. 220, Springer, 2011,