Ronnie Damonte

IT Risk Assessment:

Developing and defining the IT Risk Assessment Process Framework in the case company

Helsinki Metropolia University of Applied Sciences

Master of Business Administration

Business Informatics

Thesis

10.05.2016

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Ronnie Damonte IT Risk Assessment: Developing and defining the IT Risk Assessment Process Framework in the case company 79 pages 10th of May 2016
Degree	Master of Business Administration
Degree Programme	Business Informatics
Specialisation option	
Instructor	Antti Hovi, Senior Lecturer

The objective of this study was to define the Information Technology risk assessment process framework for an international Finnish firm belonging to a major IT corporation. The study was motivated by the fact that, in the case company, due to the lack of a common defined process for IT risk assessment, it was challenging to correctly evaluate and compare the relevancy on each risk. As a consequence, potentially misleading and inconsistent information on the impact and related importance of IT risks may have led the top management to make incorrect investment decisions.

The current state analysis was based on both qualitative (two rounds of semi-structured interviews) and quantitative (maturity survey) data. Nineteen managers and directors of the case company participated in different phases on the data collection. These data was utilized to create the project proposal, which was shared, commented and then approved by the top management of the case company. Additionally, the survey was used to evaluate the level of IT risk assessment process maturity in the case company before and after the project, as well as to compare it with industry benchmarks and the best in class.

The final outcome of the present study was the definition of the IT risk assessment process framework for the case company, leading to the following outcomes: (1) Common IT risk evaluation approach was established across the organization, and it is now duly followed in order to achieve a correct IT risk evaluation, (2) resources of the case company are used more efficiently. This is due to the fact that the top management may, on the basis of a reliable IT risk assessment, make informed decisions, concentrating the resources of the company on the most relevant risks.

In conclusion, based on the feedback and the comparison to defined targets, the research has fully achieved the established business objectives.

Keywords	IT risk assessment, IT risk management, maturity modelling

Contents

1 Introduction

In the first chapter, we will explain the reasons why IT Risk management has been chosen as the main topic of this study, provide brief introduction about the case company, and finally outline the objectives and expected outcomes of this research.

1.1 Background information

1.1.1 IT Risk Management in context

IT has deeply transformed business in different ways. Customers have fast and direct access to companies and their products and services, which makes buying as easy as clicking a mouse. At the same time, businesses can gather data about those customers far faster than any focus group could do and then analyze the numbers to determine both what those customers are likely to buy and the best way to convince them to buy it (Lainhart, 2000).

These transformations have exponentially increased the importance IT Risk Management, creating new IT risks to the business that simply did not exist before today's age of electronic communication, like privacy issues related to the management of sensible data.

So, the amount of IT risks has steadily increased over a surprisingly few years because the technology that carries the information has evolved rapidly, leaving legacy risks in place even as it creates new risks to investigate and manage (McColumn, 2011), increasing at the same time the relevancy, financial and organizational impact of these risks.

For these reasons nowadays it is imperative for companies to ensure that IT risks are adequately addressed. (Gartner, 2014)

This is particularly true for the case company, an international Finnish firm belonging to a major IT corporation, due to the industry where it operates. Besides, heading the overall IT Risk and Assurance in the same case company, I saw this thesis as a possibility to apply a structured and focused approach in improving case company's IT Risk Management process. Hence, I have selected IT Risk Management as the high-level topic for the Master Thesis.

1.1.2 Description of the case company

The case company is a Finnish multinational communications and information technology enterprise, operating in more than 150 countries and with reported annual revenues of around 10 billion USD. The company focuses on data networking and large-scale telecommunications infrastructures, concentrating in particular on mobile broadband equipment.

Thanks to the industry where the case company operates, and its focus on IT R&D development, IT Risk Management represents one of the key areas to ensure the right strategic allocation of resource, supporting top management in making informed business decisions.

1.2 Business problem

The overall needs to improve the Risk Management practices in IT department represented one of the key message that the Chief Information Officer (CIO) delivered to me as soon as I was appointed as Head of IT Risk and Assurance.

Anyway, the scope was at this point too wide to be addressed in mid terms and provide concrete results that would quickly meet expectations and tackle the most severe issues. In order to narrow the scope of my intervention, several key stakeholders were interviewed (detailed explanations of methods and tools are available in chapter 2 “Methods and data gathering”), and a questionnaire was also used to assess the maturity of the IT Risk Management practice in comparison to the industry average and the best in class.

During this analysis performed at two levels (stakeholders interview & benchmarking questionnaire) several improvement areas where highlighted, and an holistic project plan was defined in order to improve the maturity and reliability of the IT Risk Management process.

For the purpose of this research, one specific area was finally selected: the assessment and evaluation of IT Risks.

The reason of this choice is simple, its importance for the company. An adequate evaluation of IT Risks is one of the key phases that identify a mature IT risk management practice, since it defines the most relevant risks that a firm should manage.

In the case company, due to the lack of a common defined process for IT risk assessment, it was really challenging to know if the company was investing its resources into

the right risks. As consequence, potentially misleading information on the financial impact of IT Risks may lead the top management, who is at the end responsible to take decisions about how to deal with the risk, to start multi million Euros projects that may address the wrong risks.

1.3 Research question, objectives & outcomes of the research

Based on the business problem, we have defined one research question:

- How should IT Risks be assessed and evaluated in the case company?

Consequently, this paper will focus on one objective, providing three expected outcomes (see table 1):

Table 1: Objective and outcomes.

Objective	Outcomes
Define a structured approach to assess and evaluate the impact of IT Risks in the company.	**1.1.** Ensure that a common IT Risk assessment approach is followed in the company.
	1.2. Improve the likelihood of a correct risk evaluation.
	1.3 Obtain a more efficient use of company's resources, concentrating them on the most relevant risks.

More in details, these objective and related outcomes represent what the case company wish to achieve with this project research. The concrete outcome of this work will be the definition of the IT risk assessment framework for the case company, and here it is explained how this concrete output and the objectives of the organization are connected:

1.1 In order to ensure a *common IT risk assessment approach*, the case company need to have a defined IT risk assessment framework. Without a common IT risk assessment approach, top management cannot compare different IT risks, since they are evaluated based on different principles, rendering problematic to make informed decisions and to assign company's resources wisely (Reding, 2013).

1.2 The IT risk assessment process framework that is defined as result of this study will be based on established methodologies. This fact increase the likelihood that all relevant elements for a correct risk evaluation will be taken into consideration in the case company, improving at the same the *risk assessment quality and precision* (Ross, 2013).

1.3 A more precise assessment of IT risk, achieved by the utilization of IT risk assessment process framework, ensure a *better utilization of organizational resources* (both human and financial), since they will be concentrated on the most critical risks (Reding, 2013).

The defined objectives and outcomes were discussed and agreed with the CIO and the relevant stakeholders, in order to maximize the benefit of this study for the case company.

1.4 Before proceeding: some limitations

This document focuses exclusively on the IT Risk assessment process:

- Other risks other than IT are not been covered. This is because IT Risks have unique characteristics differentiating them from Operational and Financial Risks. Furthermore making a study including the overall risk landscape would have been too wide in scope, since several projects should have then been defined in order to include other categories of risks.
- Despite the fact that the definition of communication tools, techniques, stakeholders, mitigation processes for IT Risks are also part of the official company project, they will not be included in this study.
- The scope of the research will consist of only one company of the group, even though results will be freely available to the other parent companies.

2 Maturity model, benchmark and literature review

In this chapter, the selected maturity model, so a tool utilized to evaluate the IT Risk assessment process of the case company, and the relevant literature related to IT Risk Assessment are described. The aim of this overview is to provide the theoretical backbone for the final product of this study: the new IT Risk Assessment Process Framework. Additionally, the theories and models presented will offer the reader with the needed background information to achieve a correct understanding of the concepts treated in this paper.

2.1 Maturity model

The process described in the maturity model and the consequence benchmarking data will be the key element of the Current State Analysis for the case company.

2.1.1 Introduction

The maturity of IT risk assessment processes is an important indicator of the overall effectiveness and efficiency of IT risk management of an organization. Based on current studies, many companies are struggling to complete the journey toward a mature program, and in most organizations, investment in risk assessment processes lags other IT disciplines, such as operations and service management, by three to five years (Steuperaert, 2010).

Anyway, some organizations have successfully utilized process maturity metrics, comparing their own process maturity level with defined benchmarks, and implementing defined improvement strategies (Ebert, 2004). Under this point of view, an evaluation of IT Risk Assessment maturity will support the project that we are staring in three ways:

1. *The evaluation of IT Risk Assessment maturity will help the case company to identify strengths and weaknesses in its current model, comparing it a predefined structure and industry benchmark.*

   Therefore, the process maturity evaluation will be the cornerstone of the Current State Analysis, since we will be able to compare the process in the case company against established measures, defining the gaps that should be addressed (Ebert, 2004).

2. *The application of process maturity analysis will support the definition of clearly measurable goals.*

Maturity model is, by nature, numerical. It assesses the status of a process assigning to it a value (in relation to IT processes, these values are designed on a scale between 0 and 5). In this way, once the current state is numerically described, the top management will be able to indicate what target numerical value should be achieved by the project (Shanahan, 2011).

3. *The same process will provide a clear evaluation of the results of the project.*
   Since, with the maturity model, we can assess the gaps and define measurable objective, we could also utilize it to verify if those established objectives have been met. As example, a company has an IT risk management maturity model of 2, and the objective is to achieve level 3 within 12 months. In this case, re-performing the maturity assessment after 12 months provides as overall result of 3.5, meaning that the defined project exceeded the expectations (Steuperaert, 2010).

Please note that the maturity model we have utilized for the project (described in the next sub-chapter), it is valid not only for IT Risk Assessment, but for the whole IT Risk Management process. It is important to remember that the improvement of IT risk assessment is part of a larger project of overall IT Risk management enhancement for the case company.

2.1.2 Selection of the right maturity model

We selected the Gartner maturity model, in order to ensure that the project would:

a. Follow an established maturity model.
b. Provide a reliable industry benchmark for the Current State Analysis.
c. Support the verification of how well the project achieved its objectives under the maturity point of view.

There are five reasons for this selection:

1. *Gartner is one of the most established research company in the IT field*, being highly respected by technical experts and top management alike. This means that findings or action points based on Gartner model provide a strong business case once presented to IT management.
2. *Gartner maturity model is following the ISACA maturity model.* Since the Gartner maturity model is a licensed product, we can provide only the information that is available to the public. Anyway, because the basic structure is a replication of the

ISACA maturity model, the latter one can be utilized to better explain how maturity model works. . Additionally, the fact that Gartner maturity model is based on ISACA standards provides a good level of consistency in the overall theoretical approach to this research, since, as explained in this chapter, this research is built on the ISACA IT Risk framework (Gartner, 2015).

3. *Gartner maturity model includes a standard assessment questionnaire*. The possibility to employ the Gartner maturity model allows us to use the related questionnaire that Gartner has created. This save project time, since the definition of a reliable assessment questionnaire needs a considerable amount of resources, and based on cost/output calculations it saves for the company monies as well (we calculated that the cost of purchasing this product was 70% lower that the creation of a in-house questionnaire). Additionally, findings and proposed actions based on Gartner questionnaire, which was defined by a team of experts having access to large amount of technical material and companies' data, are more reliable and provided a stronger message to the management in comparison to finding based on an in-house developed questionnaire (Gartner, 2015).
4. *With the Gartner model we have access to benchmarking data,* which is fundamental in order to compare the case company with industry standards (Gartner, 2015).
5. *Gartner is already one of the case company preferred supplier,* making the purchase of this service faster than in case we would select another supplier (supplier selection process, in case of totally new supplier, may take months due to background check, financial due diligence, etc.).

2.1.3 Description of the selected maturity model

In Gartner model, process maturity represents a measure of the accountability, transparency and effectiveness of a process. Therefore, maturity assessment is essentially an evaluation of a risk management program based on indicators of maturity, which include management processes, personnel and organizational structures, technology and tools, and business culture (Shanahan, 2011).

In order to apply efficiently the maturity model several steps must be applied:

1. *Step 1: Develop a Process Catalog*

   Process formalization is the starting point for risk management process and program maturity. Organizations should:

- Develop a risk management process portfolio that represents the desired state of process environment.
- Selectively prioritize processes from this portfolio for assessment and formalization.
- Formalize these processes via ownership allocation; assessment of processes, procedures and activities; formal definition and resource allocation.

For most organizations, process formalization entails identifying, assessing, modifying, aligning and documenting processes and procedures that are at varying levels of formalization and maturity (Steuperaert, 2010).

Few, if any, organizations have the resources to implement the complete process portfolio immediately.

2. *Step 2: Assess Process Maturity*

   Program maturity is essentially a function of the maturity of the underlying processes (Astromskis, 2014). This is because program maturity reflects the status of activities that are typically manifested through processes. The de facto mechanism for measuring process maturity is an approach based on a widely recognized and consistent index: Software Engineering Institute's (SEI's) Capability Maturity Model Integrated (CMMI). In essence, this approach defines six levels of maturity that can be ascribed to specific processes, as de-scribed below (Ebert, 2004):

   a. *L0: Non existent*

      Characteristics: There is no process maturity.

   b. *L1: Reactive*

      Characteristics: In this state, the enterprise has no formal risk governance structure, risk assessments are not conducted, and senior management is not engaged in any risk management activities. There may be general awareness of the need for risk management, sometimes triggered by a specific event (such as an audit finding). In many cases, senior management risk awareness is driven primarily by media reports. Risk management is ad hoc and few individuals have defined risk management skills or responsibilities, except for traditional, compliance-centric efforts in information security.

These factors inevitably result in confusion, redundancy and conflicts of interest, with individuals doing whatever they believe is appropriate in the absence of formal directives.

Moreover, enterprises at Level 1 have extremely limited risk assessment and reporting capabilities. No formal risk assessment process is in place, and no risk register or risk management process catalog exists. Accountability is limited or non-existent, and typically rests with frontline IT professionals rather than the appropriate owners of the risk, such as line-of-business managers. Perhaps most crucially, there is no explicit acknowledgment or acceptance of residual risk by the appropriate stakeholders.

c. *L2: Developing*

Characteristics: Individual employees have received some guidance and training for their risk management responsibilities. Risk assessment is being conducted on a limited basis, and risk-related decisions are being made, but no formalized risk program is in place yet. Compliance requirements remain a primary driver of risk management decisions at this level. The lines of business and other internal organizations are broadly aware of their responsibilities, but accountability is not formalized or established as enterprise policy. An ad hoc group or groups of these individuals meet informally to discuss risk-related issues, but these discussions are at an essentially tactical level. At this level, organizations understand the limitations of their current positions and seek to extend the early support they have from senior management into budget-level and engagement-level commitments.

d. *L3: Defined*

Characteristics: This level marks the beginning of strategic planning for risk management. A comprehensive and accurate risk register has been created, and plans are beginning to be implemented to address the gaps identified at the previous levels. Exception management is formalized to track authorized deviations from policy and control requirements. Organizations relate specific risks to the impacts on specific business processes, which are the basis for mapping KRIs into KPIs.

At this level, exception management processes and the risk register are key tools for translating business needs into appropriate controls.

e. *L4: Managed*

Characteristics: The enterprise's risk management governance committee oversees multiple risk areas, including IT, operations, finance and legal/compliance. Risk-related conflicts of interest have largely been eliminated, and the enterprise's risk management efforts are now appropriately staffed by personnel with the necessary skill sets. Risk-related roles and responsibilities are clearly defined using a responsible, accountable, consulted and informed (RACI) matrix. Risk measurement is commonplace and standardized across the enterprise, and reporting is continuous. Most control gaps have been closed, and the mapping of KRIs to KPIs is formal. Sign-off of residual risk is formalized and successfully engaged for all appropriate circumstances.

At this level, the risk management program is essentially complete. Moving to Level 5 is entirely dependent on the readiness of executive management to engage in the risk management process.

Continuous improvement in the program is focused on refining the quality and usefulness of information passed to executive decision makers.

f. *L5: Optimized*

Characteristics: Risk management is now fully integrated with strategic, business-level decision making, and governance is effectively driven from the most senior levels of executive management. There is now board-of-directors' visibility into, and commitment to, the enterprise's risk management efforts. An enterprisewide, risk-aware culture now exists in which individuals and organizations are fully aware of their risk-related responsibilities. Risk assessments are conducted on a continuous basis, risk management processes are continuously improving, and exceptions are being managed effectively and within established limits.

Risk management is embedded into executive decision making in all appropriate areas. The success of the program is based entirely on the value it delivers to business decision makers.

In conclusion, this step is particularly important since it allow the case company to compare itself to the best in class (maturity level 5) and the industry benchmark provided by Gartner.

3. *Step 3: Develop a process maturity gap analysis*

The gap analysis creates a bridge between the current and the desired state, applying three relevant maturity metrics for each key process (Ebert, 2004):

- Actual state (developed in Step 2)
- Target state (developed in Step 3)
- Planned state in a given time frame (developed in Step 4)

4. *Step 4: Address the identified gaps through projects*

Based on the findings identified in the gap analysis, a set of projects devoted to address these development areas should be defined, aiming at the improvement of the maturity of the underlining processes (Steuperaert, 2010).

5. *Step 5: Define a strategic plan*

Once the top management is aware of the impact of each project into the maturity level of the process and, consequently, on the risk posture, the projects can be prioritized based on budget, schedule and impact (Ebert, 2004).

6. *Step 6: Regular Reporting*

The key to continuous top management interest in the process of viewing the organization's risk posture through a qualitative maturity assessment is ongoing engagement through quarterly reports that presents the status and related improvements of project (Ebert, 2004). A regular report will as well work as an early warning and direct escalation mechanism for in case issues would arise. Most importantly, these reports will answer one of the lost pressing questions for executives today: "How secure are we?"

In conclusion, this method of qualitative maturity assessment is a combination of process maturity, risk assessment and project management. These skills, integrated with this process, create a powerful planning and communication tool.

For this process to work, most organizations must change their culture to engage the business in caring more about operational risk and being ready to participate actively in the topic.

2.2 Key definitions in risk management

On high level, risk can be considered as a challenge to achieve the objectives defined by the organization, or, more technically, it is the combination of the probability of an event to occur and of its consequences to the business. Therefore, risk management is defined as the coordinated activities to direct and control an enterprise with regard to risks, foreseeing challenges and lowering the chances of those challenges occurring and their impact into the company (Kouns, Minoli, 2010).

The International Organization for Standardization (ISO)/International Electro-technical Commission (IEC) 31000, which states: “Risk is the effect of uncertainty on objectives. An effect is a deviation from the expected, positive and negative” (ISO, IEC 31000, 2009).

Risk management starts with understanding the organization, but the organization is mostly dependent on the environment in which it operates. Assessing the context of an organization includes evaluating the intent and capability of threats; the relative value of assets and the respective relationship of vulnerabilities that threats could exploit to intercept, interrupt, modify or fabricate data in information assets. Another relevant factor to be considered is represented by the strategy of the organization, which is setting as well the goal, providing at the same time the base for company’s risk definition (Kouns, Minoli, 2010).

The strategy of the organization, more generally, will drive the individual lines of business that are embedded in the organization, and each line of business will develop information system that support its business function (ISACA, The Risk IT Framework, 2009). Figure 1 illustrates how IT risk relates to overall risk of the organization.

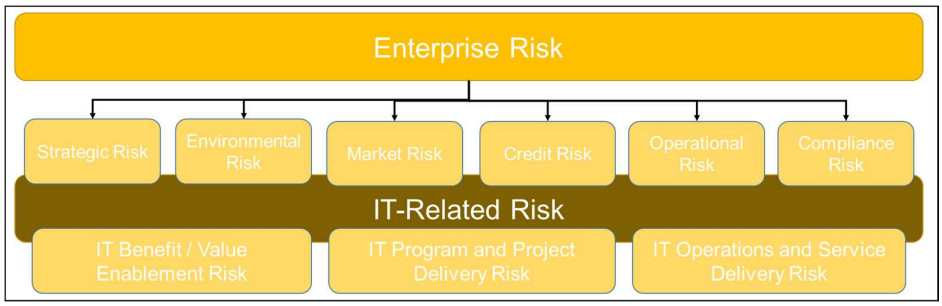

Figure 1: IT Risk in the Risk Hierarchy (ISACA, The Risk IT Framework, 2009)

Risk is an influencing factor and must be evaluated at all levels of the organization: the strategic level, the business unit level and the information system level. A properly managed risk framework addresses and takes into consideration the impact of risk at all levels and describes how a risk at one level may affect the other levels, categorizing at the same time each risk with different gradient of magnitude (the grater is the risk, the higher is the probability of loss).

2.3 Choosing the IT Risk Framework

IT risk framework is the implementation of a risk strategy that reflects the culture, appetite and tolerance of the senior management of the organization, considers technology and budgets, and finally addresses the requirements of regulation and compliance. In this way, an effective IT risk framework is critical to the ability of an organization to execute its overall business strategy in an effective and efficient manner (Kent, 2007).

Different IT risk management frameworks could have been taken into consideration for our work. After analyzing the various possibilities, the framework that chosen for the development of IT Risk Assessment Process Framework for the case company is the ISACA IT risk framework.

There are some background facts, which were the foundations of our choice:

- The ISACA frameworks is built on the following two main sources:
    - ISO31000, which is a quality standard that provides principles and generic guidelines on risk management.
    - Control Objectives for Information and Related Technology (COBIT), which is a framework created by ISACA for IT management and IT governance.
- The case company needs to comply with TL9000 IT quality requirement.
- The case company has built its IT management & governance model on COBIT and needs as well to follow Sarbanes-Oxley Legislation (an US law with the aim of reducing the likelihood of material misstatement in the financial statements via the creation and testing of internal controls procedures and activities).
- The application of ISO31000 is in accordance with the specific requirements included in TL9000, while based on the International Association of Internal Auditors COBIT is the framework that is most commonly used to comply with Sarbanes-Oxley regulation.

Consequently, based on the abovementioned background, we choose the ISACA IT risk framework for the following reasons:

- Using ISACA risk framework as a basis for our project, we can comply with the quality standard (TL9000) and the IT management & governance model (COBIT) of the case company, at the same time ensuring that Sarbanes-Oxley requirements are duly followed. This combination of advantage was not available in any other risk framework.
- Additionally, IT risk landscape, as explained in the introduction, is changing constantly. The ISACA risk framework is one of the newest framework available, having been published in 2009 and reviewed in 2012. This fact guarantee that ISACA risk framework takes into account the most recent developments in the IT risk landscape (e.g. cloud-computing) & risk management.

2.3.1 High level description of ISACA IT risk framework

The ISACA IT risk framework organizes key activities into a different of processes. These processes are grouped into three domains: *Risk Governance*, *Risk Evaluation* and *Risk* Response (see figure 2):

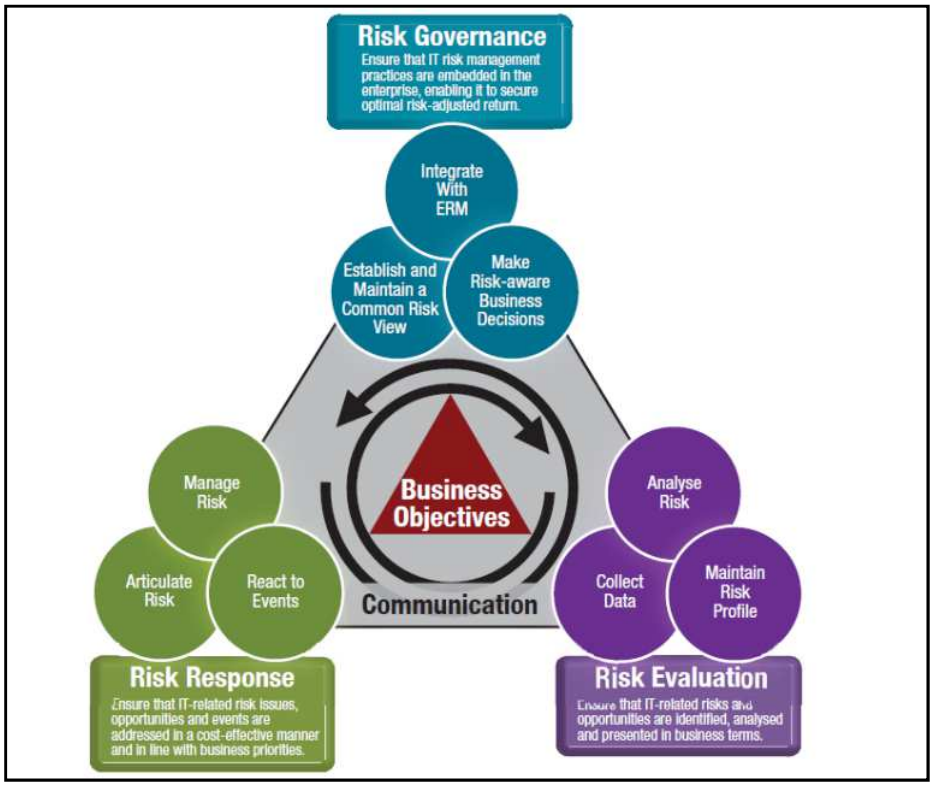

Figure 2: Risk IT Framework (ISACA, The Risk IT Framework, 2009)

The first step in the IT risk management process is the *Risk Governance* of IT risk, which includes determining the key stakeholders, the risk context, the risk framework and the process of identifying and documenting risks.
This step align with the next phase of the IT risk management process: IT *Risk Evaluation*. The effort to assess risk, including prioritization of risk, will provide management with the data required for consideration as a key factor in the next phase, risk response and mitigation.
Finally, *Risk response* addresses the risk appetite (the broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission or vision) and tolerance (the acceptable variation relative to the achievement of an objective) of the organization and the need to find cost effective ways to address risks (COSO, 1994). This phase includes as well the risk and control monitoring reporting. Controls, risk management efforts and the current risk state are monitored and results are reported back to senior management, who will determine the need to return to any of the previous phases in the process.

This IT risk management framework is based on the complete cycle of all the elements. A failure to perform, any one of the phases in a complete and thorough manner will result in an ineffective IT risk management process. In the same way, a failure in any step of the cycle may cause a deficiency that will affect the other phases. As with all life cycles, the process continues with refinement, adaptation and a focus on continuous improvement and maturity (Lainhart, 2000).

As anticipated in the introductory chapter, we are not going to analyze the whole IT risk management process, but only one of its steps: IT risk assessment, represented in this case by *Risk Evaluation* phase. In the theoretical framework explained in the following pages, I wanted to add information about the *Pre-Work* activities that, even though they are not specifically describes as a formal phase in the ISACA IT risk framework, represents an important part of the preparation of a successful IT risk assessment.

2.4 IT Risk Assessment Theoretical Framework

IT risk is a subset of enterprise risk. The risk faced by IT system is often measured by the impact of an IT-related problem on the business service that the IT system support (Iliescu, 2010). Therefore, the calculation or assessment of its impact must consider the

dependencies of other systems, departments, business partners and users on the affected IT system.

The calculation of the risk assessment is essential to provide data to top management in order allow them to make informed decisions in relation to risk response and mitigation. The choice of an appropriate response is dependent on the accuracy of the data provided from the IT risk assessment effort.

Risk assessment is defined as a process used to identify and evaluate risk and its potential effects (Reding, 2013). Risk assessment includes assessing the critical functions necessary for an enterprise to continue business operations, defining the controls in place to reduce exposure and evaluating the costs of such controls. Risk analysis often involves an evaluation of probabilities of a particular event (Kouns, 2010).

There are several well known risk assessment methodologies and standards. However, they describe the relationship between risk identification and risk assessment differently. Some standards specifically state that risk identification is a component of risk assessment (ISO/IEC 27005), whereas other standards describe the two as a separate process (IEC 31010).

The key factors in deciding on an approach to IT risk assessment are external factors, the threat situation, and the consequences of control failures. The spectrum generally runs from ad hoc techniques used by relatively low-level employees to integrated risk management throughout the technology lifecycle.
Selecting an IT risk assessment approach suited to the need involves deciding between hosts of available techniques. The decision will be based on the amount of effort required, the risks involved in the situation, and the skill set and information available to support the risk management effort. Anyway, both mainstream literature and standards agrees that using a consistent risk assessment methodology or framework is more important that which one is used (Kent, 2007). So, we can now start analyzing in details the IT *Risk Evaluation* section of the ISACA IT Risk Framework (see figure 3), chosen as theoretical framework for the case company.

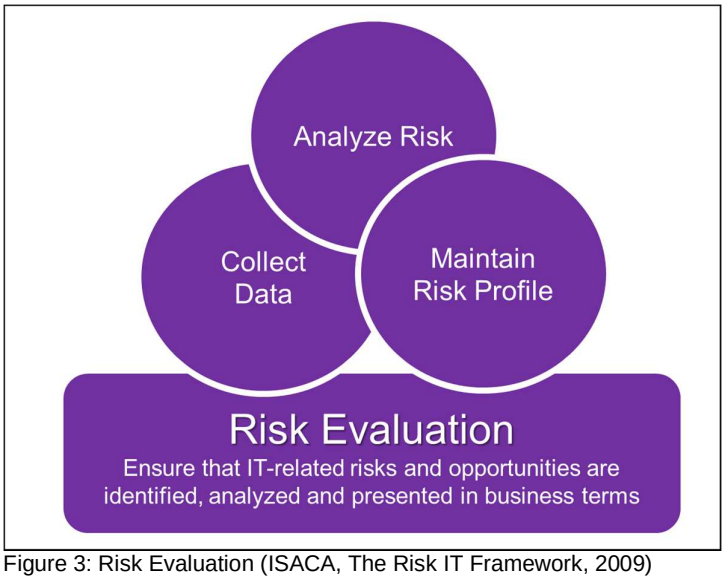

Figure 3: Risk Evaluation (ISACA, The Risk IT Framework, 2009)

2.4.1 Prework

During risk identification, risk scenarios are developed and used to identify potential risk events. These scenarios are useful to communicate with the business and gather input data required to understand the potential or probable impact of the risk event if it were to occur.

The impact of a risk event is often difficult to calculate with any degree of accuracy because there are many factors that affect the outcome of an event. If the event is detected quickly and appropriate measures are taken to contain the incident, then the impact may be minimized and the recovery process may be rapid (Nico, 2015). Anyway, if the organization is unable to detect the incident promptly, the same incident could cause severe damage and result in a much higher recovery cost. Some of the factors that can affect the calculation of risk assessment are described in the following sections (Iliescu, 2010).

2.4.1.1 Organizational structure and culture

The structure and culture of the organization or the unit under review are contributing factors in risk prevention, risk detection and risk response. A mature organization has policies, procedures and an effective reporting structure in place to detect, notify and escalate a situation effectively. An organization that does not have a mature incident response capacity will react to incidents in an ad-hoc reactive manner and will experience inconsistent results (Reding, 2013).

The risk management function should have an enterprise wide mandate that allows the risk management team to review and provide input into all business processes. They should participate in the incident management activities and e responsible for investigating incidents to ensure that all lessons are learned, in order to improve incident response planning, detection and recovery. It is important to note that lessons learned in one unit may be applicable in protecting other departments from the same problem.

If the culture of the organization is to hide problems rather than communicate or address them, then the ability of the risk practitioner to effectively contribute to the protection of the organization and assist in the investigation of an incident may be severely impaired.

2.4.1.2 Policies

Policies provides direction regarding acceptable and unacceptable behaviors and actions to the organization, sending at the same time a clear message from senior management regarding the desired approach to the protection of assets and the culture of the company. Policies give authority to the staff of the risk management, audit and security teams to perform their responsibilities. Policies should as well clearly state the position of senior management toward the protection of information. This will lead to the development of procedures, standards and baselines that implement the intent of policy and mandate that all departments comply with its requirement.

There are often several layers of policies. A high-level policy is issued by senior management as a way to address the objectives of the organization defined in the mission and vision statements. Usually high-level policies require compliance with laws and best practices and state the goals of managing risk through protecting the company's assets, including the information and IT systems that support business operations (Reding, 2013).

The next level of policies is technical and include specifics regarding the use of technology, like in the password and access policy. These policies are subjected to change, as technology evolves and new systems are developed (Kouns, 2010).

High-level policies are instrumental in determining the approach of the organization towards risk management and the acceptable levels of risks. Without policies in place, the

risk practitioner may not be able to gain access to key personnel, be left out of strategic sessions and be ignored when performing investigations.

The risk practitioner should assess the risk associated with the policy framework of the organization and provides recommendations as necessary.

2.4.1.3 Standards and procedures

Standards and procedures support the requirements defined in the policies set by the organization. A standard is defined as a mandatory requirements, code of practice or specification approved by a recognized external standards organization, such as the International Organization for Standardization (ISO). Standards are implemented to comply with the requirements and direction of policy to limit risks and support efficient business operations. The use of standards provides as well authority for the practices and procedures of the organization because a standard requires the implementation of certain practices (Reding, 2013).

Instead, a procedure is a document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes, and they are invaluable for implementing the intent of the policies (Ramamoorti, 2013). They describe in a consistent and measurable way how an operation is conducted, so that the risk practitioner can be assured that operations are performed properly and based on that abnormal activities can be detected (Kouns, 2010).

A lack of standards and procedures will result in undependable, inconsistent operations and may lead to difficulties in detecting risk events and noncompliance with regulations (ISACA, 2009).

2.4.1.4 Architecture

A key factor in the maturation of the processes and practices of an organization is the development of an enterprise wide approach to risk management, architecture and business continuity (ISO, IEC 27005, 2008). The development of an enterprise wide approach will promote consistency, repeatability, compliance, accountability and visibility to senior management into the practice and strategy of the organization (Kissel, 2009).

The systems used by most organizations have been built as part of individual projects or initiatives, and each system is an independent entity with little in common with other systems. The lack of architecture results in gaps between system ownership and unclear areas of responsibility for incidents or configuration management. The more complex and undefined an architecture is, the more challenging it is to secure the entire network and ensure compliance with safety standards, regulations and good practices (McCollum, 2010).

2.4.1.5 Controls

When assessing risk, the risk practitioner must take into consideration the current control environment. Controls are implemented to mitigate risks or to comply with regulations. However, the assessor may find that many controls are not working correctly, are poorly maintained, are not suitable in relation to the risk or are incorrectly configured (Iliescu, 2010).

A review of the controls evaluates whether the controls are working effectively to mitigate the risk and that there is the correct balance between technical, managerial, physical and operational control types. Implementation of a technical control, such as a firewall, requires correct training for the staff who will manage or operate the control, correct procedures for configuring the control, assignment of responsibilities for monitoring the control and reviewing the log data generated by the firewall, and regular testing of the functions of the control (Kouns, 2010). If adequate controls are not in place, stakeholders may develop a false sense of security, and this could lead to a serious risk of unidentified vulnerabilities or an ineffective use of resources.

2.4.2 Phase 1: Collect data

In performing a risk evaluation, there is usually a large amount of data sources available (as example network devices, application logs, audit reports), but this fact can represents a risk as much as a benefit. A too big amount of data may hide or obscure important but less evident events, and the incorrect collection of data may lead to erroneous conclusions (Kouns, 2010). Additionally, an excessive quantity of data will hinder the effectiveness of the risk analysis.

Thus, the aim of this phase is to collect and analyze *relevant* data in order to lead to an effective and efficient IT-related risk identification, analysis and reporting.

The *key actions* of “Collect data” phase are the following (ISACA, 2009):

1. *Establish and maintain a model for IT risk data collection, classification and analysis.*

   A clearly defined IT risk data collection model will support the measurement and assessment of risk attributes (e.g. availability) across IT risk domains and will provide useful data for setting incentives for a risk-aware culture.
   The risk manager should include multiple types of events and different categories of IT risk in the model, in order to ensure that it can be generally applied to the majority of potential risk cases (Reding, 2013).

2. *Collect data on the operating environment.*

   In the data collection model there needs to be a record of elements could play an important role in managing IT risks, as the change log of the Enterprise Resource Planning (ERP) environment of the organization.
   Additionally, it is necessary to review the information sources available to the business, legal, audit and compliance departments, ensuring in this way a large coverage of potential IT risks emerging in other units than IT (a good example is represented by the so called *shadow IT,* which includes applications purchased and managed by non-IT department without IT experts’ involvement).

3. *Collect data on risk events.*

   Capturing relevant information from IT related issues, incidents, problems and investigations, represents a strong starting point in order to concentrate the risk evaluation on meaningful data. Therefore, in the model, data on risk events that have caused or may cause negative impacts to IT benefits, to IT program and project delivery, and to IT operations and service delivery should be recorded.

4. *Identify risk factors.*

   For business-relevant analogous events, risk manager should organize the collected data and highlight contributing factors (as example drivers of the frequency and magnitude of risk events).

Additionally, it is relevant to determine what specific conditions existed when risk events were experienced and how the conditions may have affected event frequency and magnitude of loss, identifying in this way common contributing factors across multiple events.

Finally, a periodic event and risk-factor analysis has to be performed in order to identify new or emerging risk trends and to gain an understanding of the associated internal and external risk factors (Parthajit, 2009).

2.4.3 Phase 2: Analyze risk.

The risk practitioner must compare the current state of risk against the desired state of risk, including a review of the effectiveness of controls to mitigate risk. The desired state of IT risk is closely linked to the risk acceptance level set by the top management of the organization. Consequently, the risk manager should learn what the risk acceptance level of the organization is and then compare the current level of risk with the level of risk that is considered acceptable by the management. Where the current level of risk exceeds the acceptable risk level, the risk practitioner has to identify and document these findings and defined adequate means to mitigate them (Fenton, 2012).

In conclusion, the risk analysis is a process that guide the development useful information to support risk decisions that take into account the business relevance of risk factors.

The *key actions* of “Analyze risk” phase are the following (ISACA, 2009):

1. *Define the scope of IT risk analysis.*

   In order to identify on the expected extent and complexity of risk analysis efforts, the risk manager should first map relevant risk factors and the business criticality of assets considered to be in IT scope.

   It is important to notice that the optimal value from risk analysis efforts is obtained by favouring a scope based on productive processes and products of the business (as example revenue generation, customer service, quality) over internal structures not directly related to business outcomes (as example types of hardware, physical locations, functional organizations).

The risk analysis scope is then defined after considering business criticality, cost vs. expected value of the analysis and possible regulatory requirements (Kent, 2007).

2. *Estimate IT risk.*

   The risk manager has to estimate the probable frequency and probable magnitude of loss or gain associated with IT risk scenarios as influenced by the pertinent risk factors, and that action should be performed across the scope of the IT risk analysis. Additionally, the maximum amount of damage that could be suffered (as example a worst-case monetary & value loss in case a negative evet would occur) should be calculated, defining in this way the risk scenarios.

   Based on the most important scenarios, the risk practitioner should identify potential mitigating controls or activities, as procedures or statutory audits, that may diminish the impact of the risk.

   Based on this complete set of information, the risk manager can then evaluate the residual risk exposure levels and compare to acceptable risk tolerance to identify exposures that may require a risk response (ISO, IEC 31010, 2009).

3. *Identify risk response options.*

   The risk manager needs to take several steps in order to identify the risk response options, among which the most relevant can be defined as such:

   - Examine the range of risk response options, such as avoid, reduce/mitigate, transfer/share, accept and exploit/seize.
   - Document the rationale and potential trade-offs across the range.
   - Specify high-level requirements for projects or programmes that, based on risk tolerance, will mitigate risk to acceptable levels.
   - Identify costs, benefits and responsibility for project execution.
   - Develop requirements and expectations for material controls at the most appropriate points, or where they are expected to be rolled up to give meaningful visibility.

4. *Perform a peer review of IT risk analysis.*

   Performing a peer review of the risk analysis results before sending them to management for approval and use in decision making it is an important

step that reduce the possibility of errors and enhance the quality of the report.

2.4.4 Phase 3: Maintain risk profile

In order to ensure that the IT risks and mitigations remain relevant for the company and for the top management, it is key to maintain a risk profile or register .

This document must be regularly updated and should include the complete inventory of known risks and their attributes (as example frequency of occurrence, potential impact and disposition). Additionally, owners and IT resources involved in the risk handling or mitigating actions has to be included, enabling in this way the correct sharing of roles and responsibilities, as well a quick escalation of potential issues.

The *key actions* of “Maintain risk profile” phase are the following:

1. *Determine business criticality of IT resources.*

   The IT risk manager should identify which members of IT top management should be the owners of the identified risks. In this case, it is important to ensure the approval and the commitment of the to-be risk owners in relation to their new responsibilities.

   Clear communication of expectations towards risk owners may facilitate the communication and a successful result of the negotiation. Together with the risk owner, the IT risk practitioner can then detect the IT resources required to manage the operation of key services and critical business processes, and consequently to handle the defined risk mitigating actions response (Joseph, 2013).

2. *Understand IT capabilities.*

   In order to gain a full understanding of IT capabilities, the IT risk manager needs to follow three key activities:

   - Inventory and evaluate IT process capability, skills and knowledge of people, and IT performance outcomes across the spectrum of IT risk (as example IT benefit/value enablement, IT program and project delivery, IT operations and service delivery).
   - Determine where normal process execution can or cannot provide the right controls and the ability to take on acceptable risk (as example not

having sufficient IT project delivery capability in specific technical areas, but having strong IT program management and outsourcing capabilities, therefore, will outsource in certain cases).

- Identify where reducing process outcome variability can contribute to a more robust internal control structure, improve IT and business performance, and exploit/seize opportunities (ISACA, 2009).

3. *Update IT risk scenario components.*

   Several activities should be executed by the IT risk practitioner in order to achieve and adequate level of precision in the creation and evaluation of the components of the IT risk scenario:

   - Review the collection of attributes and values across IT risk scenario components (as example actor, threat type, event, asset/resource, timing) and their inherent connections to business impact categories.
   - Adjust entries based on changing risk conditions and emerging threats to IT benefit/value enablement, IT program and project delivery, and IT operations and service delivery.
   - Update distributions and ranges based on asset/resource criticality, data on the operating environment, risk event data (as example root-cause analysis and loss trends, real-time problem and loss data), historical IT risk data, and the potential effects of risk factors (as example how they may influence the frequency and/or magnitude of IT risk scenarios and their potential business impact).
   - Link event types to risk categories and business impact categories. Aggregate event types by category, business line and functional area (ISACA, 2009).

4. *Maintain the IT risk register and IT risk map.*

   Finally, IT risk register and the IT risk map should be updated in response to any significant internal or external change, and reviewed at least annually using the information gathered in the previous steps.

2.4.5 Theoretical framework and IT Risk Assessment implementation

Before moving on with the research, it is important to notice that we did not require specific approval for using this theoretical framework to the IT top management nor to the

steering committee defined to support the project established for implementing the IT risk assessment in the company.

The main reason for this decision is related to the way the business environment works. We are usually required to provide quick, down to earth, crisp and clear responses to top management needs. An overall theoretical framework, even though it represents the foundation of the future project, does not actually catch the attention of the top management as well as milestones project with clear deliverables.
The basics of the theoretical framework were anyway presented to the IT top management during the project initiation, as support for the proposed milestones.

3 Methods and data gathering

This chapter defines the research method used in the empirical part of this research - composed of both qualitative and quantitative data, together with the data collection gathering. These aspects represents the foundation for the research, identifying the pattern followed to achieve the objectives of this paper.

3.1 Research methods

The following mix of methods was utilized in order to gather the needed empirical data from the research:

1. First, semi-structured interviews with nineteen managers and directors of the case company.
2. A survey, represented by Gartner maturity IT risk evaluation model, to the same population as the first step with the addition of 4 IT risk management experts.
3. Finally, semi-structured interviews with three key decision makers.

Semi-structured interviews were hence used in two phases of data collection, and they were all conducted in English language.

Nineteen managers and directors were interviewed at the beginning of the research process during the first round of interviews. This initial step allowed the identification of the key areas of interests in relation to the IT risk management, ensuring that the opinion of all key stakeholders was taken into due consideration. At the same time, the involvement of relevant parties guaranteed that the consequent project would have the right internal support and funding. In addition, some questions were personalized regarding the role and responsibility area of each interviewee, in order to utilize in the best possible way the unique knowledge of each individual participating in the interview round. This is due to the fact that interviewees were coming from different organizations, having a different level of expertise in IT risk management and power of influence in relation to the direction to take to develop the area under scope.

The second round of interviews was run after having analysed the results of the Gartner maturity IT risk evaluation model. Based on the first interview round and the outcome of the maturity survey, a project proposal was prepared and presented to three selected key decision makers. The aim of these interviews was to obtain top management comments and approval on the proposed scope to be tackled by the research, getting the commitment, at the same time, of the resources needed to complete the project.

In addition to these methods, the Gartner maturity IT risk evaluation survey was utilized in order to gain numerical understating of the current overall status in IT risk management in the case company, as well as for comparing it to best in class and industry benchmarks.

Hence, a mix of qualitative and quantitative research methods has been applied in conducting this research. Quantitative research lies on the logic of positivism, typical to natural science investigation. For a long time, the quantitative research methods were considered as the way of doing research (Glesne & Peshkin, 1992). The qualitative research has its origins in anthropology and it is based on an interpretivist paradigm. In qualitative research, the data is often observed as one entity (Alasuutari, 2008). Therefore, the choice of research methods is related to how the researcher sees and understands the world (Glesne & Peshkin, 1992). Glesne & Peshkin also recognize that even though much discussion has taken place on which paradigms or methods are better, a variety of approaches has virtue. According to Glesne & Peshkin, different approaches permit us to know and understand different things about the world.

Marsland (1998) provide different possible approaches for combining the quantitative and qualitative research. The research described in this paper corresponds to a combination that Marsland (1998) call “Sequencing”. They describe the approach as follows:

- Using participatory techniques in exploratory studies to set up hypotheses, which can then be tested through questionnaire based sample surveys.
- Choosing a random sample and conducting a short questionnaire survey to gain information on key variables, which are then investigated in-depth by participatory enquiry.

In the following paragraphs, the data collecting methods of this research are explained more in detail.

3.2 Semi-structured interviews

According to Ritchie & Lewis (1981), a semi-structured may be suitable for the following reasons:

1. It provides the opportunity to generate rich data.

2. Language use by participants was considered essential in gaining insight into their perceptions and values.
3. Contextual and relational aspects were seen as significant to understanding the perceptions of others.
4. Data generated can be analyzed in different ways.

The description of Ritchie & Lewis (1981) is suitable to this research, since we need to obtain detailed data from the interviewees, in order to define specifically the areas to be reviewed and to obtain later on feedback on project proposal. Additionally, the relationship aspects, and the dependencies between teams, processes and individuals, are as well a key aspects of the planned interview. Finally, it is indeed true that the gathered data can be analysed with a wide range of techniques.

It is relevant to note that different variations exist of semi-structured interviews, and, specifically in this research, we utilize a variation called “theme interview”. The theme interview is focused on certain themes that are then discussed. Specific questions are planned in order to gain clarification of the chosen themes. The order of the questions may vary, as well as the way in which these questions are asked. Also the number of questions varies based on the how much information the interviewee gives on a single question. The interviewer should facilitate the flow of information and motivate the interviewee. In order to do this, flexibility is required both in the use of verbal and non-verbal language, as well as in the control of situations (Alasuutari, 2008).

The interviewees of both sessions participated on a voluntary basis. The purpose of the interviews was reviewed in the beginning of each session and eventual questions about the scope were answered.

3.2.1 First round of interviews

Nineteen managers and directors of the case company were interviewed in the first phase of data collection (see Table 2), representing seven different units. The interviews took place during November 17, 18, 19, 20 & 21, 2014 at the premises of the case company, and lasted about one hour each. All interviews were conducted either as face-to-face meeting, or via online meeting tools.

Table 2: Description of the first interview round

Position	Organization	Interview length (minutes)	Type of interview
Head of Corporate Risk Management	F&C	60	Face to face
Head of Internal Controls	F&C	55	Online meeting
Head of Internal Audit	F&C	45	Online meeting
Head of Risk Management & Resilience	Health, Safety and Security	60	Face to face
CIO	IT	60	Face to face
Head of CIO Office	IT	60	Face to face
Head of IT Security	IT	58	Online meeting
Head of Software Assets Management	IT	45	Online meeting
Head of IT for Central Functions	IT	50	Face to face
Head of IT Partnering Management	IT	60	Online meeting
Partnering Manager	IT	60	Face to face
Program Manager in Transformation	IT	60	Face to face
Head of IT Integration Services	IT	60	Face to face
Head of Privacy	Legal	55	Face to face
Head of Indirect Software Procurement	Procurement	50	Face to face
Global Category Manager	Procurement	45	Online meeting
Senior IT Quality Manager	Quality	45	Online meeting
Head of Quality IT	Quality	60	Face to face
Head of Supplier Management	Supplier Management	56	Online meeting

There were specific reasons for choosing these interviewees, teams and units. Each of the seven units identified has a strong linkage or dependency on IT risk management:

- Finance & Control unit owns the overall risk management topics, and the most relevant teams that deals with IT risk management analysis are the following:
    - *i. Corporate Risk Management:*

      It owns the overall risk management topic at corporate level, providing guidance and setting the expectations in this area.
    - *ii. Internal Controls:*

      Risks are taken into consideration once defining new controls, and often the risk mitigating activities are overseen by Internal Control.
    - *iii. Internal Audit:*

In the annual audit planning, a fundamental element for the scoping definition is represented by the results of risks analysis. Additionally, audit results may be start or be included in risk assessment programs.

- Health, Safety and Security in *Risk Management & Resilience* team reviews IT risk management data, in order to plan resiliency (business and service continuity management) related activities.
- The *Privacy* unit in Legal has a strong linkage to IT risks, since nowadays no data can be managed in a large company without adequate IT infrastructures and IT services. Due to the importance of the subject, Privacy issues may feed IT risk, and IT risks may be included in legal privacy considerations.
- *Indirect Software Procurement & Supplier Management* may be involved in handling some IT risks, because specific IT tasks are outsourced to external service providers.
- IT risk mitigations are often part of project with the aim of enhancing internal capabilities and improving processes. For this reasons, the view of *IT Quality* on IT risk management is important to ensure that the positive part of risk management, so called opportunity management, is taken as well into consideration.

The single interviewees were chosen because of their role as leaders of their respective areas, or because their deep technical understanding of IT risk management.

Objectives of the first round of interviews can be summed up as follows:

- Identify of the key potential improvement areas in relation to the IT Risk Management.
- Increase the awareness of the top management on IT risk management topic.

3.2.2 Second round of interviews

The second round of interviews was carried out on December 10 & 15, 2015, after the survey results had been analysed. In this phase three managers were interviewed (see Table 3). The interviews were conducted at the premises of the case company.

Two interviews took place on December the 10th, in order to get comments and commitment before meeting finally with the CIO on December the 15th. In the meanwhile,

amended version of the project proposal were created based on the feedback received, and sent back for approval.

Table 3: Description of the second interview round

Position	Organization	Interview length (minutes)	Type of interview
Head of Corporate Risk Management	F&C	120	Face to face
Head of Risk Management & Resilience	Health, Safety and Security	120	Face to face
CIO	IT	90	Face to face

We had multiple aims of for this second interview:

- Explain the Gartner maturity model explained, in order to ensure a common understanding of the model, of the industry benchmark, and of the overall results for the case company.
- Present the overall results of the interviews and the survey.
- Define the right maturity level in different areas (including IT risk assessment) for the company based on the Gartner model.
- Obtain comments and final approval on the proposed project scope and plan.
- Define a first list of Steering Team members for the project.
- Gain additional development ideas from the top management.

The three interviewees were chosen since they are key decision makers in their own area of responsibility, able to approve the level of budget and resources needed to manage this kind of project at global level.

As anticipated, the interviews with the Head of Corporate Risk Management and with the Head of Risk Management & Resilience took place before the meeting with the CIO. This is due to the fact that the CIO is the ultimate owner of IT risk management, and I needed to ensure full support from Finance and Control and from Health, Safety and Security units before presenting the status and the proposed solutions to the CIO.

The results of both set of interviews are described in chapter 4 as part of the AS IS analysis.

3.3 Surveys

This subchapter discusses the characteristics of a survey as a research method and describes the data collection process that was carried out through a survey for this research.

Survey as research method means a type of study in which the focus is on the data that looks at the present situation (Gerring, 2007). Survey data is empirical and it contains the assumption that the phenomena are measurable. A detailed general view on the research topic is attempted to be formulated through a survey. The data in a survey is collected mainly through a questionnaire or an interview. When a questionnaire is used, it is often both standardized and structured. The structuring refers to the quantity of open or closed questions in the questionnaire. In a structured questionnaire ready-made options exist for all the questions. The standardization means the level of steadiness of the questions in the questionnaire, both related to the form and order of the questions. (Alasuutari, 2008).

Based on the definitions provided, the survey used for this research can be considered standardized. The data was collected through an electronic survey developed by Gartner that the selected managers and directors could access online.
Aim of the questionnaire was to perform a risk management maturity assessment, understanding in this way weaknesses and strength of the IT risk management process of the case company and comparing it to the industry benchmark and best in class. At the same time, it also help confirming or not the elements that emerged from the first interview round. Since Gartner questionnaire is a licenced product, the detailed description of its content will be omitted from this paper.

The questionnaire was open for answers between November 22, 2014, until December 4, 2014, to all the managers and directors included in the first interview round, with the addition of 4 IT risk management experts from IT unit.
Two reminders were sent: one on November 27, 2014, and the other on December 2, 2014. The questionnaire language was English. The total number of the managers that received the questionnaire was 23, of which 22 answered, resulting in 96% response rate.
As for the results of the interview, the data that emerged in the survey it will covered as part of the AS-IS analysis performed in chapter 4.

In conclusion, this chapter has presented the methods used in the present research, discussing at the same time the theoretical background and reasoning behind their selection.

4 AS-IS analysis

In this chapter the current IT risk assessment process overall status will be analysed, explain at the same time the results of the interview and the Gartner survey. Additionally we will present the defined target state for IT risk assessment maturity defined by the top management of the case company, outlining the project designed for that purpose.

4.1 Data collection and analysis

As described in chapter 3, in order to gather the needed data to define the scope of the research, analyze the current state in the case company and obtain the needed support from the top management, we followed three steps:

1. Semi-structured interviews with nineteen managers and directors of the case company.
2. Gartner maturity IT risk evaluation survey, to the same population as the first step with the addition of 4 IT risk management experts.
3. Semi-structured interviews with three key decision makers.

We can now present what have been the outcomes of the first two phases.

4.1.1 Results of the first round of interviews

The aim of this step was to identify the key areas of interests in relation to the IT risk management, gaining as well a broader view on the topic, its dependencies and potential plans already in place for the development of this area.

Despite few differences across units, due to the different level of involvement in IT, the most common comments and concerns of the interviewees can be summarized with the following examples:

- *"No IT risk management improvement programs had been carried out in the case company after 2010. Before that, the only noticeable project is represented by the implementation of a risk management practice between 2004 and 2006. The area has been totally neglected." Head of Privacy.*
- *"IT risk management process documentation is scarce and out to date." Head of CIO Office.*
- *"Communication to top management on IT risks and related mitigation is ad-hoc based, and lack continuity, clarity and focus." CIO.*

- *"There is no predefined IT risk management scoping, which would guide the development actions in the area." Head of Corporate Risk Management.*
- *"No methodology has been established for risk assessment and evaluation. We do not know if we are spending our budget wisely" CIO.*
- *"No-one knows the costs of the risk mitigation activities, which means that we have no idea about the ROI of these actions for IT and the case company overall." Head of IT for Central Functions*
- *"Roles and responsibilities are not clear, and they are several overlaps." Head of Indirect Software Procurement.*
- *"Risk awareness is low across the IT unit, leading to poor attention to risk management and the implementation of agreed mitigations." Head of IT Security.*

Even though what has been listed are examples of comments gathered during the interview, they represents at the same time common ideas across the population of interviewees. Therefore, based on the first interview round, we found that the most valuable potential areas of improvement in IT risk management were the following:

1. Reporting.
2. Process.
3. Risk awareness culture.
4. Tactical plan and budget.
5. IT risk assessment.
6. Domain scope.

The fact that so many areas of IT risk management necessitate deep and strong improvement project it also means than the overall maturity of this process is low.

Additionally, since the areas are so many, we really needed an analytical tool and data in order to select the key areas to invest the case company resources. For this reason we moved then to the second step of the data gathering: the Gartner IT risk management survey.

4.1.2 Results of the survey

The utilization of Gartner IT risk management survey had two specific aims: confirm the area of research identified during the unstructured interviews and provide a benchmark against best in class and industry standards.

Even though the Gartner questionnaire is analyzed in chapter 2, figure 4 provides a recapitulation of the different maturity level for overall IT risk management.

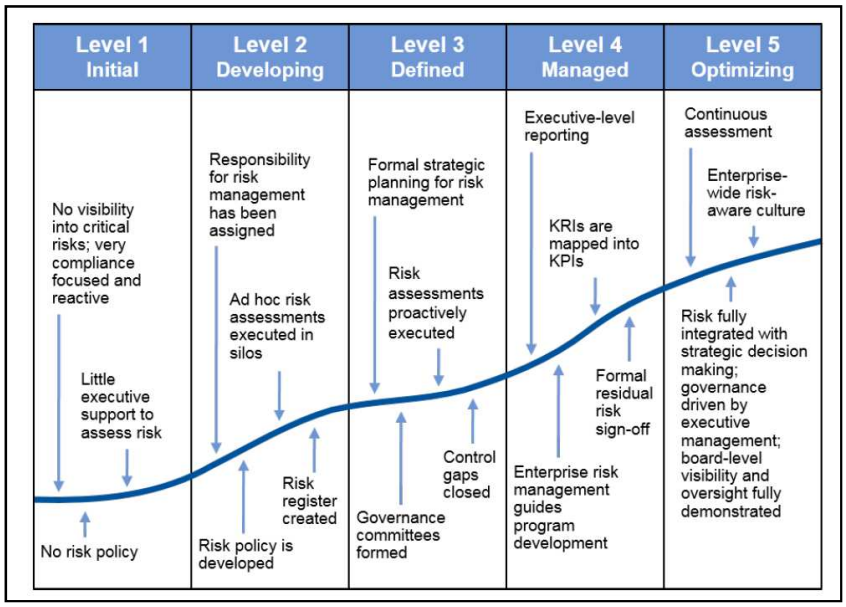

Figure 4: IT Risk maturity levels (Gartner, 2015)

In the survey, each relevant IT risk management area has a dedicated set of questions and maturity levels are provided for each area and for IT risk as a whole.

The questionnaire maturity results will be shared only for IT risk assessment, the topic selected for this topic. Anyway, it is worth mentioning that out of six improvement topics identified during the first round of interviews, only three were selected based on the survey. Those were the areas where the different in comparison to the industry benchmark was most significant. IT risk assessment was part of this group.

4.2 IT risk assessment status

The Gartner survey section dedicated to IT risk assessment covers three key subjects:

1. Topic 1: The utilization of specific IT risk assessment methodologies.
2. Topic 2: The formalization of IT risk assessment processes and procedures.
3. Topic 3: The financial evaluation of IT risks and related mitigations as part of T risk assessment.

Therefore, figure 5 shows the maturity level that the interviewees assigned in the questionnaire to IT risk assessment, based on their evaluation of each of the three topics assigned to this area. Additionally, Gartner questionnaires describes the IT risk assessment maturity status of the case company in comparison to best in class and benchmark.

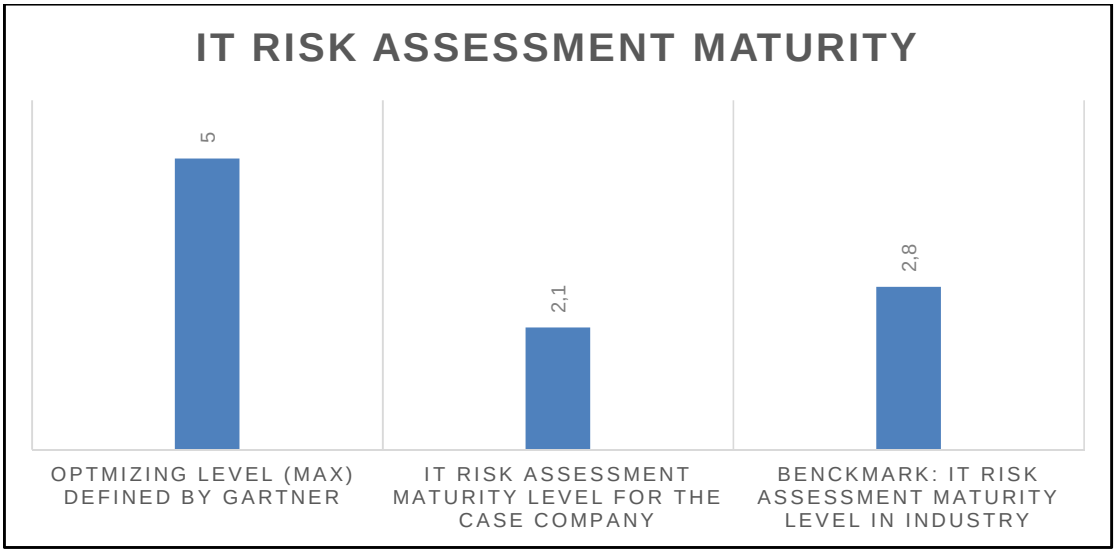

Figure 5: Maturity level in IT Risk Assessment for the case company.

This result means that the case company had reached a general *L2 developing* maturity in IT risk assessment, which is clearly worse that the industry benchmark (closer to a *L3 defined* maturity level). It is as well clear that in order to achieve best in class level *L5 optimizing* in the case company would require strong top management commitment to invest time and resources in this area.

Based on the first round of interview, on the answers to the survey and the observation of the case company risk management environment, following reasons have caused a 2,1 maturity level scoring in IT risk assessment:

- *An IT risk assessment framework is not applied in the case company.*

Even though methodologies are defined for managing IT units and services in the case company, no framework has been defined for IT risk management and consequently on IT risk assessment. The consequence is represented by the fact that the case company is not following a recognized and defined approach in IT risk assessment. It is then extremely difficult to evaluate the quality and the reliability of the assessment performed on single IT risks. Additionally, there may be consequence for the case company under the IT quality and legislative point of view; as example ISO27005 requires organizations to define and choose an adequate IT risk assessment methodology (ISO/IEC 27005, 2008).

- *IT risk assessment process and procedures are not described.*

  In this kind of situation, top management cannot compare different IT risks, since they are evaluated based on different principles, rendering problematic to make informed decisions and to assign company's resources wisely.

- *Only some IT risks present a financial evaluation, while no mitigating activities present a budget and an analysis of their effects on the IT risk impact.*

  Due to lack of a common IT risk management process it is impossible to evaluate the correctness of the financial impact assigned to IT risks, making it challenging to know if the company is investing into the most relevant risks. Additionally, the lack of defined monetary evaluation of mitigations and its effects on the risk may lead to a sub-optimal allocation of resources. For example, there could be cases where a 5 million euros project could lead to a 4 million euros positive effect on the risk, which of course would not make sense. At the moment of the questionnaire, there was no way to perform this kind of comparison.

Since the root cause of these broader issues in IT risk assessment were due to the lack of a well-recognized, structured and defined IT risk assessment process framework, we defined a project in order to ensure the definition of the IT risk assessment procedure in the case company.

4.3 Proposed target state

Before starting defining the overall project plan, timeline, resources and outcomes, the target state needed to be established. All the project actions would have then been directed to the achievement of the target state.

Based on the maturity definition, the high level information gathered on the current state in the case company, and on the current projects in the risk management area, the following strong target was proposed to the top management:

- *To achieve maturity level L4 Managed in IT risk assessment within one year.*

The reasoning behind that target are the following:

- The case company has the competences, resources and ambition to achieve that target.
- Level L4 Managed in IT risk assessment could provide a boost in the overall maturity level of IT risk management, leading to a competitive advantages against case company close competitors. Due to the line of business of the case company, a well-managed IT risk environment could represent a strong selling point for certain clients.
- Under the decision making point of view, level L4 Managed provides to the top management an excellent degree of visibility and clarity about IT risk evaluation & costs.
- At this maturity level, mitigations are financially evaluated, and their impact on risks is regularly assessed, ensuring more focused investments and efforts for the case company.
- It is an excellent maturity level in order to evaluate the opportunity and need to move eventually towards level L5 optimizing. Even though it is the best in class maturity level, not all organization needs such an advanced IT risk assessment status. Additionally, trying to move directly to L5 optimizing was an high risky move due to the extremely low maturity level in the case company. Metaphorically, it is better to do your degrees step by step, instead of moving directly from junior high school to the doctoral degree.

4.4 IT risk assessment project: high level description

In order to achieve this target maturity level in IT risk assessment, we defined a project divided in four phases:

1. *Data collection.*

   Aim: Obtain the necessary data in order to plan the project, including scope, targets, timeline and resources. Receive the necessary feedback, support and approval to start the project.

   Description: This phase was included in project description despite the fact that was already ongoing. It is represented by the three different data gathering stages (first interview round, survey, second interview round) described in chapters 3 and 4.

2. *AS-IS Analysis.*

   Aim: Define in detail what the current IT risk assessment status is in the case company.

   Description: Utilizing the material obtained in the first phase, present technically the IT risk assessment cycle status to the top management & project steering.

3. *Theoretical Framework.*

   Aim: Collect the theatrical base for the IT risk assessment framework to be built in the case company.

   Description: In this phase all the relevant material for definition the new IT risk assessment methodology in the case company is collected and discussed. At the same time additional industry references are presented

4. *Definition of the new process*.

   Aim: The IT risk assessment process framework is defined and approved.

   Description: This phase start in parallel with phases two and three, since the IT risk assessment process framework is defined based on the information, feedback and analysis gathered along the project.

A schematic view of the project is presented in figure 6:

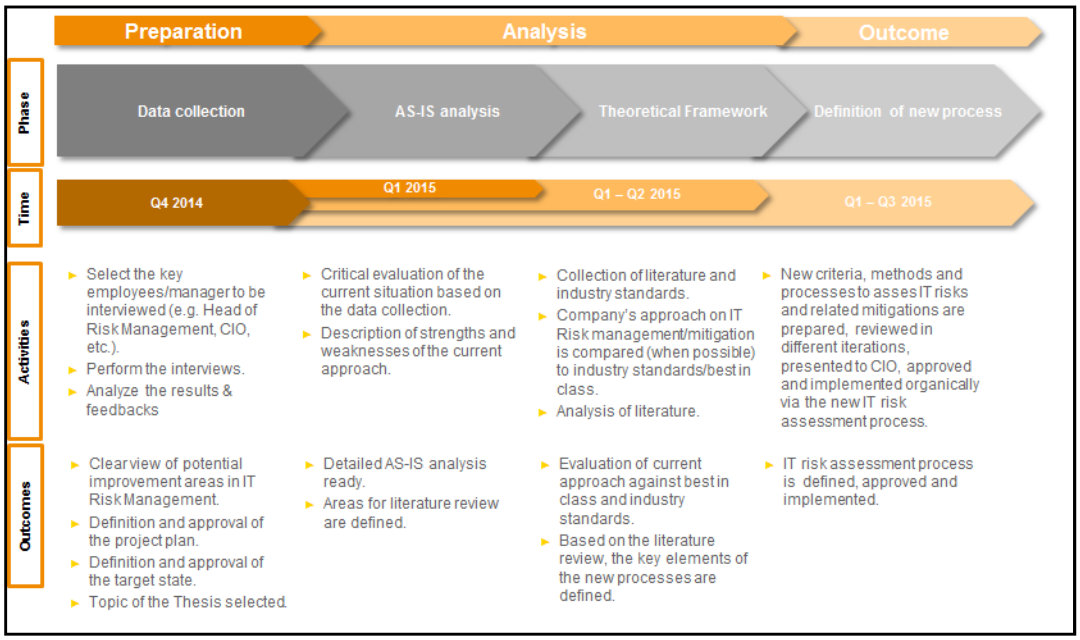

Figure 6: IT risk assessment project.

At the end of the project, another survey will be launched in order to assess the maturity level in IT risk assessment, evaluating in this way the results of the project against the target goal.

Both the proposed target state and the possible project designed to improve this area were presented to three key decision makers in the case company to gain the needed approval and funding.

4.5 Project approval and definition of target state

In order to obtain feedback on and approval to the target state and project proposal, I interviewed three key decision makers:

- Head of Corporate Risk Management from Finance and Control unit.
- Head of Risk Management & Resilience from Health, Safety and Security unit.
- CIO from IT unit.

The interview took four phases:

1. In the first phase, the Gartner maturity model was explained, in order to ensure a common understanding of the model, of the industry benchmark, and of the overall results for the case company.

2. After that, the proposed target state and the reasoning behind that was presented. At this point we started an open discussion about the proposed target and what means we could utilize to achieve it.
3. Then, the high level project proposal was described, and we compared it to the suggested actions discussed in phase 2.
4. Finally, an official approval was requested.

The final results of this interview round were the following:

- All agreed on the proposed target state. Based on the feedback received is was solid improvement goal, challenging but reachable at the same time. There was also full agreement about the fact that level L5 optimizing it would have been too difficult, costly and time consuming to achieve for the case company at the present moment.
- The proposed project was also approved, with the caveat about the theoretical framework. Basically, everyone agreed on the need to have a strong theoretical framework, at the same time it was agree that only the final product, the IT risk assessment process framework for the case company, would have been presented. The basic theoretical framework would have been mentioned, but they saw no need to present a detail analysis to the steering committee and to the top management.

On the basis of this approval and feedback, the project lead to the definition of the new IT risk assessment process framework described in chapter 5.

5 Definition of the new standards

In this chapter, we defines the framework for planning and conducting IT risk assessments that was created for the case company in order to achieve the research objectives. Additionally, the feedback iterations with the key stakeholders and the overall outcomes that the introduction of the IT risk assessment has brought to the case company are described in the following pages, in order to provide a holistic overview of the process followed and its final results.

5.1 Approach in the definition of IT risk assessment process framework

The fundamental aim of the process presented in this chapter is to provide a structured and pragmatic approach that provides consistency of execution while being flexible enough to encompass a variety of types of assessments, methodologies and tools.
In order to achieve this objective, there is a large number of industry frameworks that can be used for structuring risk management and assessment programs. Anyway, the most prevalent and widely recognized are the COBIT and ISACA, described in the literature review. The IT risk management principles followed in COBIT and ISACA are consistent with both the overall Risk Management of the case company, as well as with the requirements of the external auditors, which must be taken into consideration in this are for possible regulatory compliance demands.
Additionally COBIT and ISACA frameworks have a proven track record, since they have been applied by several originations that aimed to achieve goals similar to the ones set up by the case company in this area.

These considerations have brought the project team to utilize both the COBIT and ISACA frameworks in order to define the IT risk assessment process for the case company. The defined approach is built, nevertheless, also on own consulting and professional experience in this field and on the regular input and feedback from the steering team and key stakeholders.

5.2 The IT Risk Assessment Process Framework

As stated in the introduction, the key stakeholders in the case company had set the following expectations for this project:

1.1 Ensure that a common IT risk evaluation approach is followed in the company.

1.2 Improve the likelihood of a correct IT risk evaluation.

1.3 Obtain a more efficient use of company's resources, concentrating them on the most relevant IT risks.

The IT Risk Assessment Process Framework address the managements' expectations, since it guides assessors in the whole company through the steps that are required to maximize the effectiveness of assessment activities, increasing the likelihood of a successful result, at the same time providing a consistent global approach throughout IT. The by-product of these combined elements is an enhanced risk evaluation, which, in our plans, will allow the top management of the case company to make more informed decisions, resulting in a better use of firm's resources.

So, the framework comprises the following components (one pre-work and 5 phases), as shown in figure 7:

0. Perform the pre-work.
1. Phase 1: Gather the requirements
2. Phase 2: Structure the IT risk assessment
3. Phase 3: Execute the IT risk assessment
4. Phase 4: Phase Review, assess and change
5. Phase 5: Communicate

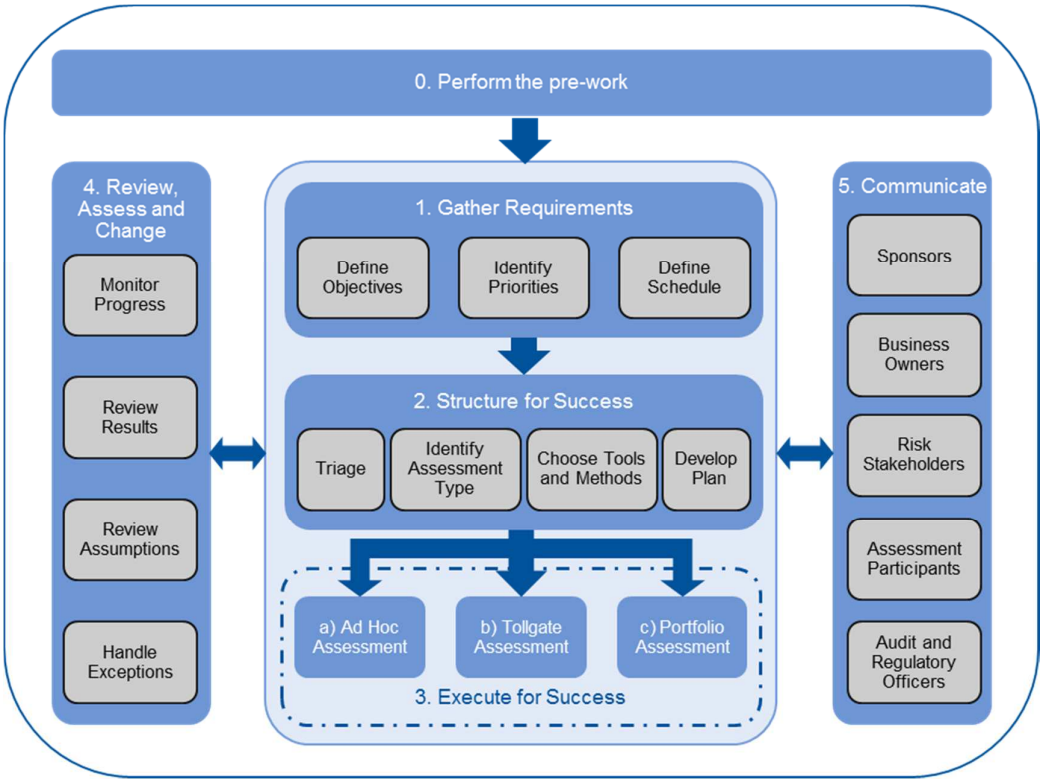

Figure 7: IT Risk Assessment Process Framework

For each of those process phases we have identified key activities and critical success factors that should lead to a successful planning and executing IT risk assessments.

In the rest of the chapter, we will go through every framework component, in order to provide a cleat overview to the reader of the process structure and of what has been considered in preparing the detailed process material. Nevertheless, we are not entering into the details of the framework material, in order to avoid risk of leaking relevant information to competitor of the case company.

5.2.1 Perfom the prework

IT risk assessment is conducted within the overarching IT risk management program. The IT risk management program has been defined as part of this project, and it provides the direction and the boundaries for the IT risk assessment activities. Therefore, a successful IT risk assessment must be planned and executed within a broader context that will influence and guide the evaluation activities.

The following types of information from the IT risk management program and the broader organization are relevant in setting the context and preparing for all IT risk assessments:

- Policies, frameworks, methodologies and tools that are used for IT risk management and IT risk assessment within the organization.
- Risk criteria that are defined by the case company, including:
    - The types of threats and consequences to be considered.
    - Vulnerability information.
    - How IT risk likelihood and impact will be measured.
    - How levels of risk will be defined.
    - The level of risk (also called risk appetite) that is acceptable by the company.
- Key roles and responsibilities within the organization that are stakeholders of the assessment outcomes.
- Decision-making processes and reporting lines within the organization that may influence the collection of information and the reporting of assessment results.
- Key external drivers that affect the organization, including the competitive landscape, business objectives, market trends and technology developments.
- The requirements of external stakeholders, including legal and regulatory requirements.
- The capabilities and experience of the resources to be assigned to the assessment.
- The objectives and success criteria of the IT projects or processes that are targeted by the assessment.

5.2.2 Phase 1: Gather the Requirements

Phase 1 is focused on the definition of the specific IT assessment to be undertaken within the context defined in the Pre-work stage. A successful IT risk assessment must be defined and scoped within the broader risk management context that is established in the Pre-work. For those undertaking IT risk assessment activities, this step is critical to ensuring that the assessment scope and objectives are well-defined, business and assessment priorities are clear, and critical deadlines are understood.

The *key activities* of Phase 1 are the following:

- *Define the scope:*

    A clearly defined scope for an IT risk assessment is critical to ensuring that the assessment can be completed and that the results will be acceptable to the assessment owners and sponsors. Typically, in the scope items that

need to be specifically included or excluded from the assessment are indicated, as well the type of assessment to be conducted, and the drivers for the assessment.

- *Understand priorities and business criticality:*

  It is unlikely that an IT risk assessment will be the top priority across an organization. The assessor must understand where this assessment fits within the broader organizational priorities, in order to be able to engage stakeholders, get commitments and develop a sensible schedule. For example, an assessment that must be completed before other activities can commence (such as a merger) will be on that effort's critical path. On the other hand, an IT risk assessment that is scheduled as part of the annual risk management program may be seen as a lower priority.

- *Agree to deliverables and time frames with sponsors*:

  There is wide range of deliverables that could be produced from an IT risk assessment. Understanding the deliverables that are required will influence the activities undertaken. Timeframes for conducting the assessment will be influenced by a large number of factors, including, as example, priorities and business criticality (as discussed above), availability of stakeholders, and assessment resources.

The *critical success factors* for Phase 1 are the following:

- *Level of engagement of sponsors and owners:*

  IT risk assessments are generally perceived as disruptive to project and operations work. Consequently, having a clear sponsor aids in winning the respect and commitment of participants. Additionally, because sponsors are generally people who want to have the IT risk assessment completed, they will be responsible for negotiating timeframes and deliverables as well as supporting the assessment activities within the organization. It is also important to determine who the owner is for the assessment results. In some cases, this may also be the sponsor, but it may as well be business owner within the organization where the IT risk assessment is performed.

- *Trade-offs between scope, time frames and resources have been agreed upon:*

  Agreement, evidenced via documented sign-off, on scope, time frames and available resources is essential. If timeframes are too tight or if there is lack of resources, then the assessor must evaluate the reduction of the scope.

Alternatively, if the scope is fixed, then it is essential to negotiate for additional resources or a deferred delivery date.

- *A clear and actionable statement of the business objectives of the assessment has been developed, and the sponsor has signed off on it:*

  This statement can be used throughout the assessment to confirm that activities and findings remain on the agreed track. The success of the assessment can be easily measured based on the achievement of these objectives.

5.2.3 Phase 2: Structure a Successful Assessment

Phase 2 is the detailed planning stage, which is critical for ensuring that the assessment is performed in the most effective and efficient way.

At first, in defining the detailed planning, the assessor should leverage from the information gained in the Prework stage and from the requirements outlined during Phase 1. This is an important step, but it is anyway not sufficient in order to structure an effective assessment. To achieve this goal, the work must be planned in such a way that the proposed effort is appropriate for the risks under consideration. In the same way, the assessor needs to select methodology and tools that are appropriate to the assessment that the organization is undertaking. As example, a relatively minor IT risk assessment task should not be overwhelmed by a complex methodology.

The *key activities* of Phase 2 are the following:

- *Perform a triage:*

  One of the most valuable preparatory activities for an IT risk assessment is to prioritize the work to be conducted. The recommended approach in the prioritization is to perform an initial high-level assessment, or triage, to quickly determine the relative business value and importance of the assessment items in order to rapidly structure and prioritize the work. This initial assessment could take the form of a business impact assessment to highlight the most susceptible areas of the business. Alternatively, a sensitivity analysis could be performed for understanding the areas of largest potential impact. In conclusion, this activity should result in a clear ordering of work for the assessment.

- *Identify the type of IT assessment:*

  In the IT Risk Assessment Framework defined for the case company, we have identified three main categories of IT risk assessment that will guide the development of the work plan and the definition of the detailed activities.

  These categories of IT risk assessment are defined below:

  - Ad hoc assessments:

    These are one-off or special-purpose assessments that may be requested following particular events, such as security incident, audit findings, compliance failures or technological innovation. It is essential that ad hoc assessment results are incorporated into the higher-level risk management program, even though they are conducted outside the routine risk management process. The challenges of the ad hoc assessment for the assessor can include very short time frames, a lack of information or certainty about threats, vulnerabilities and likelihood estimates, and a different audience from regular risk assessments. Examples of ad hoc assessments include evaluating infrequently made decisions (such as the selection of new technology platforms or operations sites), assessing risk associated with business-led activities (such as developing new services or products), and assessing risk associated with major external events (such as physical disasters or new laws or regulations).

  - Tollgate IT assessments:

    These are assessments that are required to be undertaken as part of another organizational process, with a strong IT component. The most common processes where IT risk assessment tollgates is often included are procurement processes, project management methodologies and change control programs. The risk assessment in this context is generally intended to answer a yes/no or go/no-go decision. Examples of tollgate assessments include the evaluation of new

applications or services as part of IT projects and the assessment of technology risks that are associated with new supplier relationships.

- IT portfolio assessments:

  These are scheduled assessments that are usually identified during the annual risk management planning. These assessments will generally target a group of assets that are owned by a line of business, which employ common technologies. The portfolio approach to these assessments enables portions or samples of these asset groups to be regularly assessed. Often periodic assessment may utilize already existing assessments, which must anyway be reviewed, validated, updated and modified in order to meet the scope of the portfolio assessment. A challenge for practitioners undertaking these types of assessments is to ensure that changes from previous assessments are well-articulated and that the impact of these modifications is clearly identified in the assessment results. Common portfolio assessments include the assessment of IT service data protection risks, the assessment of the business impact of disasters on enterprise datacentres, and the evaluation of data protection capabilities of suppliers with access to restricted information.

- *Select the methodology and tools:*

  The assessor should select the right methodologies and tools depending on the type of assessment. Reviewing similar or related IT risk assessments that have been conducted by the organization in similar cases can provide an indication of the preferred assessment methodologies to be designated. Having a clear understanding of the required deliverables from Phase 1 and the type of assessment from the previous part of Phase 2 will also provide guidance on the selection of methodologies and tools.

- *Develop the work plan and timeline:*

  The project management knowledge, resources and structure of the case company provides the assessor with a consistent approach in developing

the project plan, in scheduling work and in identifying resource requirements. The plan should clearly identify critical path activities, dependencies and resource requirements.

- *Track and communicate progress:*

  During the project, we have defined the IT Risk Assessment dashboard, which help in track actions and communicate the progresses. The communication to management must follow a phased approach, in order to enable managers to provide feedback, comments and to address problems timely. For example, you may consider communicating status in such a way that the first of communication round will be addressed to line managers, and then include the next level of management in a second stage. This allows managers to follow-up issues and discuss delivery problems with their leaders before having executives come down on them.

- *Ensure availability of resources:*

  People are a key consideration for all assessments; consequently, ensure that the individuals and groups whose participation will be required are available, that they have the right skill mix and that they understand the importance of the effort.

- *Establish in advance how risk items will be identified, collected, classified and tracked:*

  A risk register or repository should be utilized in order to document risk issues that are identified during the assessment process. The risk register should contain all the following:

  - A standardized set of information on each item or issue.
  - A risk-scoring method that can enable prioritization and classification of the item.
  - Clearly identified ownership of the item.
  - The ability to document risk treatment plans (if appropriate) or the decision that was made on the item.
  - Finally, the ability to use workflows to ensure both a consistent process and timely actions.

The *critical success factors* for Phase 2 are the following:

- *Assessment activities and items have been prioritized properly:*

Determining top priority focus areas helps the assessor in defining the correct structure and order for the assessment activities. The triage process may be used for prioritization and for validating assumptions.

- *Planned effort is appropriate for the risks and available resources:*

  The assessing team must ensure their planning include the appropriate amount of effort for the assessment. The triage process could be applied to assess high-value assets, high-likelihood threats and significant impacts. Assessment activities should be structured and planned so the largest investment of resources is devoted in the most critical areas.

- *The methodology and tools are matched with the assessment objectives:*

  Correctly identifying the type of assessment (ad hoc, tollgate or portfolio) will help the team to structure a successful assessment. Once the assessment type has been defined, the appropriate methodology should be selected. In many cases, in IT risk evaluation the organization under assessment will have adopted a methodology fitting different assessment types.

5.2.4 Phase 3: Execute a Successful IT Risk Assessment

The execution phase of the IT risk assessment process comprises three core activities:

- Risk identification:

  This activity involves identification of threat sources, potential impacts and types of consequences. Sources of information and personnel that can assist with this activity should have been identified during the earlier phases. The threats has to consider all events that could cause some form of harm or damage. Depending on the scope defined on Phase 1, it may relate to assets, processes or performance objectives.

- Risk analysis:

  This activity focuses on understanding risks, providing the input for the evaluation and subsequent treatment of risks. Analyses of threat sources, size and type of consequences, and the likelihood of those consequences occurring are undertaken. The level of detail required in the analysis is driven by the required outcomes, which are defined in Phase 1.The decision to use a qualitative, quantitative or hybrid approach to risk analysis is made in Phase 2 when the practitioner determines the assessment type and methodology.

- Risk evaluation:

  This activity involves a comparison of the results of the risk analysis with the risk criteria identified during the Pre-work stage. The application of a wider risk context will provide the basis for recommending approaches to treating risks, including reducing, accepting or transferring risks. The risk evaluation activity may also identify the need for a further detailed analysis or a further assessment to be initiated on items outside defined scope of the current assessment.

All risk assessments will involve the three activities identified above. However, different types of assessments will bring a different focus, emphasis or perspective. The following sections concentrate on the unique aspects of executing each type of IT risk assessment.

5.2.4.1 Phase 3a: Execute a Successful Ad Hoc Assessment

Ad hoc assessments (see Table 4) are often performed in new areas for an organization and support the evaluation of strategic decisions, such as the development of new product capabilities, entry into new markets, or the adoption of new technologies or business practices. Often, ad hoc risk assessments are initiated to provide deeper insight into items that were identified by other processes or events.

Note that many risk issues that are discussed at the executive or board level will have an ad hoc analysis performed on them. Normally, items of such significance are examined and explored at greater depth than would be accomplished by using an operationalized risk assessment process.

Table 4: Sample Ad Hoc Assessments

Sample Assessment	Subject Matter	Objectives
Item analysis	Projects and processes	Develop a deeper understanding into a risk item that has been identified either through another risk process or because of an external event.
Adoption of a new technology	New technology or IT strategy	Report on the specific IT risk and control requirements for the appropriate adoption of a new technology or strategy. Many organizations have performed ad hoc assessments on their adoption of

		mobile devices, bring your own device programs, cloud infrastructure as a service, etc..
Acquisition of, or merger with, another organization	The evaluation of one or more candidate organizations for the acquisition activity	The IT risk component of an acquisition tends to have a dual purpose. The first purpose is to evaluate the technology that will be acquired with respect to how it supports the final business function. Sometimes, this is as simple as evaluating if the data is of sufficient quality to be migrated to the successor organization. The second purpose is to evaluate the characteristics of the other organization in general terms to identify secondary opportunities.
Policy exception	Exception requests to various IT policies, such as password strength and anti-guessing measures	Often, ad hoc assessments will be performed when an exception to an IT policy is requested. A common example of this situation is when an application or service uses password strength and anti-guess strategies that are different from the explicit criteria in the written policy. An exception to any policy must include an analysis of the risk that is associated with granting the exception and a determination of whether the risk is within the tolerance of the enterprise or requires a control treatment plan.

The *key activities* of Phase 3a are the following:

- *Make the risk identification and analysis processes as extensive as the scope allows:*

  Because the ad hoc assessment can be driven by a wide variety of organizational requirements, it is important to ensure that the assessing team identifies sources of risk, areas of possible impact and their potential consequences. In the same way, they need to ensure the risk analysis is able to cover the wide-range of risk sources, which may be relevant for an ad-hoc assessment. Because the ad hoc assessment is a one-off activity (unlike the tollgate or portfolio assessment), it may not be impossible to leverage previous risk assessment work. Consequently, different information sources, both internal and external to the organization, should be included in the analysis.

- *Maximize opportunities for business input to the risk evaluation process:*

  Ad hoc assessments are primarily driven by business requirements, rather than security or compliance needs. Because of that, it is necessary to ensure that business stakeholders get sufficient opportunities to input to and to comment on the risk evaluation process. In order to maximize the value brought by the business stakeholders into the assessment project, we must remember that they may not be frequent participants in risk evaluations and they may benefit from some additional explanation of the purpose of the activity, of the process followed and of the expected outcomes.

The *critical success factors* of Phase 3a are the following:

- *The right result has been achieved rapidly:*

  Due to the urgent nature of ad hoc assessments, the team will need to ensure that the time is organized in the most efficient way, in order to deliver the final report within the agreed timeframe. For this reason it is important to get agreement and buy-in from the key stakeholders on what the critical contents of the final report are. In this way assessors can limit the concentrate resources on the defined critical aspects, further improving the speed of execution.

- *Details are available to support all report findings:*

  Since ad hoc assessments are often presented to executive management, the assessors must understand and handle all the details related to the assessment project, even though these details are not specifically included in the final report. As example, if an estimate business impact is reported, then the presented should know who provided it, how they determined it and which methods have been used to calculate it.

5.2.4.2 Step 3b: Execute a Successful Tollgate Assessment

Tollgate assessments are performed in support of larger projects within governance and risk management. This is generally accomplished by injecting a process tollgate that requires the risk assessment to be completed with the results that determine whether the tollgate can be considered passed or not. Generally, the focus of the tollgate assessment is to determine the following:

- Bottleneck or constrains are present and justify an immediate response.
- Sufficient risk assessment information has been collected to support governance and risk management decisions.
- The risk evaluation determines that the risks are at a level where a "go-ahead" or approval is anticipated, perhaps with some further remediation required.

Just as with all other tollgates that are built into processes, tollgate assessments need to satisfy the tollgate criteria. Certain tollgates can be performed in parallel with other efforts, but it must be understood that relevant issues can be discovered, resulting in the cancellation of an effort or requiring compensating controls to be deployed. As a result, tollgate assessments should be performed as early in the process as possible. For these reasons organizations may implement multiple tollgates in the same process, such as performing a lightweight screening of projects prior to the finalization of key deliverables (for example, a charter, requirements or implementation planning) (see Table 5).

Table 5. Sample Tollgate Assessments

Sample assessment	Business processes that the assessment supports	Objectives
The data protection and IT service availability of a supplier	The selection of third party suppliers	Understand the IT risks that are associated with giving service providers access to sensitive and/or critical data, and ensure that suppliers are not provided data that they are not equipped to protect as well as ensure that they are able to support business process availability requirements.
Application or service security controls	The delivery of new software or services into IT via internal projects	Evaluate new applications and services to understand the IT risks, and ensure that data is properly protected and that controls are appropriate.
Screening for risk and compliance issues	The IT budget process for proposed spending on projects and products	Identity IT risk issues that could alter the feasibility or cost structure of particular proposals.
Screening for risk and compliance issues	The IT budget process for proposed spending on projects and products	Identity IT risk issues that could alter the feasibility or cost structure of particular proposals.

Sample assessment	Business processes that the assessment supports	Objectives
The evaluation of the security and control implications of new technologies	Enterprise architecture	Provide risk and security insights to support the appropriate adoption or maintenance of technology by enterprise architecture
IT project risk assessment	The IT project management office	Assess the risk of all projects, while at the proposal stage, and identify data protection, availability and regulatory compliance risks to the extent that they can be addressed during the project itself and included as requirements.

The *key activities* of Phase 3b are the following:

- *Start the risk identification activity as early as possible:*

  In an ideal world, risk issues would be addressed in advance of reaching the tollgate, so that the tollgate assessment would be a quick and simple verification step. Achieving this requires looking upstream into the process and seeking opportunities to embed risk awareness early. For this reason, assessors should partner with groups that are upstream of the tollgate to educate them about the risks that the tollgate assessment should consider and why.

- *Use information from the overarching process to inform the risk analysis:*

  The information needed to conduct a risk analysis may have already been defined in the process. The utilization of the available information and resources avoids then redundancies and duplication of work.

- *Remember the context of the overarching process in the risk evaluation:*

  Since the primary purpose for the tollgate assessment is to satisfy the requirements of the overarching process, it is critical that the risk evaluation activity include a particular focus on the context of that process.

The *critical success factors* of Phase 3b are the following:

- *Assessment participants are willing and engaged:*

  Typically, people participate in tollgate assessments because they have to. However, educating participants about the business and risk context can promote a positive interaction where those individuals understand the

value of their participation. Simple statements such as "Reducing the risk of fraud to the company and our customers" or "Ensuring that patient information is handled ethically and meets compliance requirements" can make a required compliance tollgate assessment much more palatable to participants as well as result in a smoother and more effective process.

- *Factors are identified that improve the efficiency and effectiveness of the tollgate assessment:*

  Tollgate assessments are usually performed several times through the execution of the process. Because of this aspect, it is possible to collect information on the effectiveness of the tollgate within the process, continuously seeking ways to both improve its efficacy at reducing risk and its impact on the enterprise.

5.2.4.3 Step 3c: Execute a Successful Portfolio Assessment

Portfolio assessments are performed on a set or collection of assets or entities. Portfolio assessments are often executed on an annual basis to support enterprise risk management or compliance objectives, often as response to high-impact events. For example, after Hurricane Katrina in 2005, many enterprises performed IT risk assessments of their data and business operations centers. After the threat associated with the portfolio of locations was well understood, many organizations orchestrated a portfolio assessment on all new prospective locations (assessing changes to the portfolio rather than revaluating the portfolio itself every year).

Examples of portfolio assessments are outlined in Table 6.

Table 6. Sample Portfolio Assessments

Sample Assessment	Population to be Assessed	Objectives
Financial reporting application testing and change procedures	Applications that process or supply data into systems that generate financial statements regulated by the Sarbanes-Oxley Act (SOX) legislation.	Understand the IT risks that are associated with modifying business-critical applications to ensure (1) that the financial reporting systems of the organization are tested whenever changes are made to the system or its operating environment and (2) that only approved and tested changes are made to production.

Sample Assessment	Population to be Assessed	Objectives
Data-handling practices	Branch offices and operations centers	Ensure that IT policies and standards for safe processing, transportation and storage of customer data are appropriate. Evaluate if existing controls are appropriate, given changes in business practices or expectations. Evaluate the IT risk that is associated with compensating or special-control situations.
Disaster preparedness	Data centers and locations that are critical to business operations (including those of key third-party service providers)	Ensure that disaster recovery plans are adequate, given changing business operations practices or expectations. Furthermore, ensure that the plans are not in conflict with one another or that they contain dependencies that are unrealistic.
Supplier data protection	Third parties with custody of or access to regulated or sensitive data	Suppliers change their systems and practices continuously. When these suppliers are in possession of or have access to regulated or sensitive information, then the enterprise must ensure that its data protection practices are within risk tolerance and are appropriate, given any regulatory or contractual obligations. In these situations, enterprises will often perform an annual portfolio assessment where they (1) identify suppliers with access to restricted or sensitive data, (2) collect information on the nature, volume and scope of the data in question, (3) query the supplier regarding its data protection practices and (4) assess whether the supplier is operating within risk tolerances.

The *key activities* of Phase 3c are the following:

- *Consider the whole portfolio in regard to risk identification:*

  Even though the portfolio assessment will focus on only one segment of the population at a time, it is critical that each assessment considers the

characteristics of the whole portfolio. The value of the portfolio assessment is represented by the fact that it takes a sample of the population, after which the results can be considered more broadly for the portfolio. For these assessments to be more useful than just a point-in-time assessment, the risk identification activity needs to be comprehensive so as to be applicable across the portfolio — or at least to enable the subsequent analysis and evaluation to be extrapolated.

- *Leverage prior assessments during risk analysis and evaluation:*

  Portfolio assessments are performed periodically. Consequently, it makes sense to leverage previous assessments within the portfolio to inform the risk analysis and evaluation activities. In some cases, the effort may be reduced to performing a comparison of previous data, identifying the differences and focusing effort there.

The *critical success factors* of Phase 3c are the following:

- *The assessment forms part of an overall risk assessment program:*

  Even though a single risk assessment is performed, a portfolio assessment is always part of a longer-term program of assessment activities. Where appropriate, the practitioner should consider the results of previous assessments for the portfolio, which could be used as well to support the definition of results and findings. Additionally, the assessor should verify the possibility to leverage tools available to overall risk assessment program, such as risk registers, as a relevant source of information.

- *The full population has been clearly identified:*

  Key to a successful portfolio assessment is to ensure that all the items in the portfolio have been clearly identified.

5.2.5 Phase 4: Review, Assess and Change

This phase is conducted in parallel with phases 1, 2 and 3. It includes activities that are necessary to successfully manage end to end the risk assessment process.
The assessment should be consider as any other project, and consequently well-established project management practices may help in handling the assessment.

One of the most common issue in managing IT risk assessments is represented by the fact that information collected during the assessment can fundamentally alter either the

scope or the material understanding of the assessment efforts. The discovery of unanticipated threats may lead the assessor to change the approach and scoping in order to cope with the new situation. For this reason, it is relevant to conduct regular review in the project and document its modifications.

The *key activities* of Phase 4 are the following:

- *Monitor not only the progress of the assessment, but also the information that is being collected:*

  It is important to ensure that assumptions in areas such as scope, span and impacts continue to be valid throughout the assessment project timeline.

- *Monitor regularly the data for unanticipated issue:*

  This is a key activity, in order to allow the organization to timely act in case of problem arises.

The *critical success factors* of Phase 4 are the following:

- *Regular status meetings are occurring:*

  Following standard project management practices, regular meetings must be scheduled with sponsors and stakeholders so that assessment status and eventual problems can be discussed. Additionally, it is desirable to establish in advance that issues requiring discussion will come up during the assessment process, to allow the audience to be adequately prepared for the meeting.

- *Exceptions are identified, analysed and treated as required:*

  Determine if any of the data collected or findings made alters scope, requirements and mission of the assessment. These findings and data are analysed, in order to determine the potential consequences within the scope of the assessment requirements. Additionally, assessors should be tracking these items throughout the assessment to identify which one them are relevant enough for escalation and/or remediation.

- *Resource constraints are proactively identified and managed:*

  Assessor should consider whether resource constraints such as availability and cost will have any impact on scope, timelines or quality. In case constraints are expected, a contingency plan should be defined for successfully executing the assessment.

- *Out-of-scope items are identified and managed:*

The data collected during the assessment is analysed regularly, in order to ensure that the project is proceeding within its scope. It is possible that assessor will uncover important information during the assessment, information falling anyway outside the agreed scope. The advisor will need to consider whether the scope should be adjusted to include this new material or if these data could be utilized in future reviews. In both cases, management and relevant stakeholders must be adequately informed, providing as well comments and guidance on the best way to

5.2.6 Step 5: Communicate

Communication is possibly the most important step in the IT Risk Assessment Process Framework. This phase encompasses the activities that are necessary to successfully communicate with all participants and stakeholders in the IT risk assessment process. For those undertaking IT risk assessments, this step is critical for ensuring that all stakeholders in the assessment are engaged, informed and consulted and that they are supportive of the activities and results. Throughout the assessment process, communication is required, with a range of roles within the organization and for a variety of reasons. A failure to communicate effectively can lead to poorly defined or incomplete requirements, a lack of critical information, a lack of support for findings and recommendations, and a waste of assessment effort and resources.

The *key activities* of Phase 5 are the following:

- *Communicate with sponsors:*

  The communication with the sponsors for the assessment is critical at the start of the process to ensure that the assessing team understand the requirements and correctly define the scope. Additionally, regular status updates should be provided, including unexpected or potentially controversial results. Because assessors may need to rely on your sponsors to gain the support of others in the organization, it is essential that the sponsors are informed and supportive.

- *Engage with business owners:*

  Because the business owners ultimately are responsible for assets and risks covered by the assessment, it is essential that they are involved with

and committed to the assessment. Key information and resources required for the assessment will need to come from the business owners, so without their support, it is really difficult to successfully complete the assessment. The right approach is to engage early with the business owners, seek their input and agreement to the requirements and scope, and then ensure that they are aware of progress. The results from the assessment should be clearly communicated in a separate, business-focused report or presentation, with particular emphasis on the consequences for the business of the risks identified and any recommended remediation.

- *Engage with risk stakeholders:*

  All organizations deal with different types of risks, and these are usually managed by different parts of the organizations. However, it is essential that all assessment activities are shared with and visible to all risk areas. During the assessment, risk managers throughout the company should be treated as stakeholders. In some cases, this may be limited to notification of the intent to conduct the assessment (including the scope) and then the sharing of final results and recommendations. In other cases, much more frequent and detailed communication may be required where activities have the potential to overlap or conflict.

- *Involve all assessment participants:*

  Participants may be able to offer insights that have not occurred to the assessment team, due to their deep knowledge of the area under review. For this reason, participants should receive key information such as the objective of the assessment, how it may support the company and their work, what kind of timetable is going to followed and how much support is expected from them.

- *Report to audit, compliance and regulatory officers:*

  In many cases, IT risk assessments are being conducted due to audit, compliance or regulatory requirements. Consequently, it is essential that the assessment meets those requirements. Thus, involving audit, compliance and regulatory officers in the development of scope and work plan will ensure that the assessment covers the necessary ground and will be completed in a suitable time frame. Any unusual or unexpected results should be timely shared with audit, compliance and regulatory officers. These results could have significant consequences that need to be carefully managed.

The *critical success factors* of Phase 5 are the following:

- *A communication plan has been developed that is suitable for all stakeholders:*

  Effective engagement with stakeholders and support from sponsors and owners rely on clear and informative communication about the IT risk assessment. Communication about the purpose, progress and outcomes of an assessment should always be clearly linked to the requirements defined in Phase 1. Furthermore, timetable for communication is defined to ensure that stakeholders are given notice of activities, kept informed on progress and given insights into early results.

- *Methods for communicating final results and recommendations are suitable for all stakeholder*s:

  Assessors must determine how they want to present final results and recommendations. They should consider all possible audiences for the assessment, with particular attention to the needs of the sponsor and owner. Although a detailed report is almost certainly a deliverable from the assessment, they need to consider the value of presentations, walk-throughs and executive focused summaries for the audience, in order to tailor the message.

- *Significant results are communicated early:*

  Any results or findings that differ significantly from what was expected should be clearly identified, and escalated. In the same way, positive results should be timely shared and highlighted as well.

5.3 Feedback and iterations

5.3.1 Steering committee definition

Due to the importance and relevancy of the resources allocated to the project, a steering committee was named.

The definition of steering committee members was agreed with both the CIO (Chief Information Officer) and the Project Management Organization (PMO) office, in order to guarantee adequate support from relevant units, strong decision-making, and the right mix of expertizes.

The following participants were defined as member of the steering committee (see Table 7) :

Table 7: Participants in the project steering.

Position	Organization
Head of Corporate Risk Management	F&C
Head of Internal Controls	F&C
Head of Internal Audit	F&C
Head of Risk Management & Resilience	Health, Safety and Security
Head of IT Security	IT
Head of IT Partnering Management	IT
Head of IT Integration Services	IT
Head of IT Risk and Assurance	IT
Head of Quality IT	Quality

5.3.2 Feedback and iterations

The steering team meetings were held on a monthly basis in accordance to project schedule.

Each milestones of the project needed to be approved officially by the steering committee, following the steps defined below:

1. *Proposal*: the project team would propose the closure of the project milestone, providing supporting documentation and deliverables.
2. *Feedback / Approval*: Based on the documentation provided, the steering committee would either:
    a. Approve without comments:

        The project team would consider the milestone achieved, proceeding consequently with the next planned phase.

    b. Approve with comments:

        In this case the project team, before starting the next planned phase, must work on the feedback received revisiting and modifying the material. The answers to the comments / modification of deliverables is then reviewed in the next steering committee meeting.

    c. Rejected:

> Finally, the project team would have to rework a large part of material and deliverables, in order to satisfy the steering committee requests and feedback. The approval would then be gathered in the following steering committee meeting.

This process was followed in all project milestones, until the approval of the final milestone and the conclusion of the project.

It was extremely important to have this kind of continuous and structured feedback. Thanks to steering committee comments, we were able to improve the deliverables to a level that would satisfy our stakeholders and units.

Additionally, the final deliverables and the results of the project were presented to the CIO that provided extremely positive feedback – considering as well the challenging objectives designed for this project.

5.4 Project results

After three months since the end of the project and the consequent implementation of the new IT Risk Assessment Process Framework in the company, we launched again the same questionnaire that was provided before the start of the project, applying as well the same population of interviewees.

So, after the implementation of the new IT Risk Assessment Process Framework, the maturity level in IT Risk Assessment had moved from 2.1 (status before the project) to 4.2 (status after the project) out of a maximum of 5.
The result in comparison to industry benchmark (2.8) was as well extremely positive (please see figure 8).

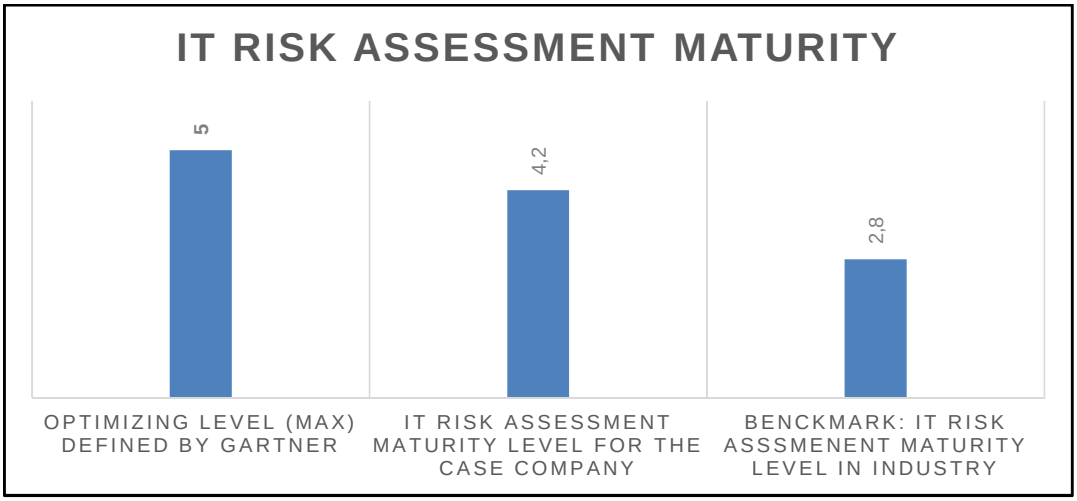

Figure 8: Maturity level in IT Risk Assessment for the case company.

Overall, it means that we exceed the target settled by the top management, which was 4.0 – managed status as defined by Gartner. It is interesting to note that to the business in which the case company is engaged, having a high maturity IT Risk Management represents a competitive advantage.

Based on the outcome of the questionnaire, the new IT Risk Assessment Process Framework and related level of maturity provides the following outcomes:

1. Common IT risk evaluation approach across the organization.
2. The detailed procedure to be followed in order to achieve a correct risk evaluation.
3. A more efficient use of company's resources. This is due to the fact that top management may, on the basis of a reliable IT risk assessment, makes informed decisions, concentrating the resources of the company on the most relevant risks.

In conclusion, the project and consequently this research has fully achieved the established business objectives.

6 Overall conclusions

This chapter concludes the work by summarizing the research project and by bringing together the main results of this research, as well as its limitations. First, we will recapitulate the research project. Then the practical implications, which are considered to be the results of the IT risk assessment project in the case company, will be discussed. Finally, the trustworthiness of this research, its limitations and the suggestions for future studies will be discussed.

6.1 Research summary

The purpose of this study was to define the IT risk assessment process framework for an international Finnish firm belonging to a major IT corporation. The study was motivated by the fact that, in the case company, due to the lack of a common defined process for IT risk assessment, it was challenging to evaluate and compare the relevancy on each risk. As consequence, potentially misleading and inconsistent information on the impact and related importance of IT risks may have led the top management to make incorrect decision, as example approving multi million Euros projects that may address the wrong risks.

In order to develop the IT risk assessment process framework, we followed a defined project plan, including the phases described on Table 8:

Table 8: IT risk assessment project description.

Project phase	Objective	Main activities
1. Data collection	Obtain the necessary data in order to plan the project, including scope, targets, timeline and resources. Receive the necessary feedback, support and approval to start the project.	In this phase three different data gathering stages (first interview round, survey, second interview round) were implemented.
2. AS-IS Analysis	Define in detail what the current IT risk assessment status is in the case company.	Utilizing the material obtained in the first phase, present technically the IT risk assessment cycle status to the top management & project steering.

Project phase	Objective	Main activities
3.Theoretical Framework	Collect the theatrical base for the IT risk assessment framework to be built in the case company.	In this phase all the relevant material for definition the new IT risk assessment methodology in the case company is collected and discussed. At the same time additional industry references are presented
4. Definition of the new process	The IT risk assessment process framework is defined and approved.	This phase start in parallel with phases two and three, since the IT risk assessment process framework is defined based on the information, feedback and analysis gathered along the project.

In each phase of the project several iterations for approval and feedback were defined with top managers, experts, key decision makers and the project steering team.
This communication flow was the single most important element that lead to reaching the established objectives for this research. Through the feedback and the input of the identified stakeholders, the team was able to improve the project execution along the way.
Additionally, involving key decision makers created the preconditions to receive the needed support for the project across the organization.

During the development of the study, the most challenging aspect was represented by a complete reorganization in IT Unit at every level, which occurred during the project execution. This means that more than half of the individuals, who were part of the project network, were allocated to different team, acquiring then different responsibilities. This aspect did not received enough attention in the project planning.
Despite the difficulties in losing the major part of the project network, we were able to regain quickly momentum thanks to the support and commitment provided by IT top management.

6.2 Overall results of the study

At the beginning of the research, one objective and three outcomes where defined (see Table 1, as described in the introduction):

Table 1: Objective and outcomes.

Objective	Outcomes
Define a structured approach to assess and evaluate the impact of IT Risks in the company.	**1.1.** Ensure that a common IT Risk assessment approach is followed in the company.
	1.2. Improve the likelihood of a correct risk evaluation.
	1.3 Obtain a more efficient use of company's resources, concentrating them on the most relevant risks.

These outcomes where linked, as explained in chapters 4 and 5, to a defined maturity level in IT risk assessment of "L4 managed" which was set as the target of the project. According to Ebert (2004), among the outcomes of a L4 maturity level, we found the ones described for this study.

Based on the final Gartner assessment, the maturity level of the case company in IT risk assessment reached 4.2 after the project. This means that the initiative did exceed the target. Additionally, the feedback received from both the steering committee and the CIO on the project deliverable (the IT risk assessment process framework) was exceptional.

In a more practical terms, we can say that the present research achieved its objectives and outcomes, for the following reasons:

- The new approach for assessing IT risk was defined in detail.
- The IT risk assessment process framework has become part of the case company internal methodology. For relevant roles, obligatory training must be received on this subject. These two elements ensure that the IT risk assessment process framework is duly followed in the company.
- All IT risks were re-assessed based on the new framework, providing consistency in the approach and enabling management to compare the impact and relevancy of any IT risk.

- Based on the new IT risk assessment executed across the organization, a review of mitigation projects was performed by the IT top management. This action had the consequence to freeze certain initiative, and invest in other consider to address more relevant risks, ensuring a more efficient use of company's resources.

In conclusion, in both technical (under the maturity point of view) and practical terms the study has achieved the desired aims.

6.3 Trustworthiness of the research

In this subchapter the trustworthiness of the present study is discussed in the light of the used methods and data.

According to Shenton (2004), development of early familiarity with culture of participating organizations contributes to the credibility of the research. Therefore, I explain here my familiarity with the case company: I am leading the IT Risk and Assurance team in the case company since 2014. I have both designed and managed IT risk management, internal audit and compliance projects in the organization. Additionally, I represent the owner for the overall IT cycle in the corporation, under the process, control and risk point of view. These roles and responsibilities have enabled me to gain a deep understanding of the IT risk management issues and opportunities in the case company. Of course, this status quo allowed me to have access to the corporate top management and decision bodies in the organization, as well as to ensure adequate support for the research and parallel project development and implementation.

The use of multiple data-collection methods contributes to the trustworthiness and validity of the research (Glesne & Peshkin, 1992). According to Guba (1981) and Brewer & Hunter (1989), the use of a combination of different methods compensates for their individual limitations and exploits their respective benefits. Marsland (1998) argue that in particular the combination of quantitative and qualitative approaches increases the trustworthiness of a study. A mix of different methods has in fact been used to conduct the present research, including both quantitative and qualitative methods. Semi-structured interviews were done in two different instances. Data was collected with a survey prepared by one of the biggest player in the industry of IT analytics (Gartner) from a sizable group of managers and directors.

Marsland (2000) define this combination of methods “enriching” from the trustworthiness aspect.

As example, the practice of undertaking qualitative studies before quantitative ones has been standard practice in mainstream market research for at least 30 years (Marsland, 2000). The Association of British Market Research Companies (ABMRC) provide following reasons for this: “Prior to any large-scale quantitative study particularly in a relatively unknown market, it is strongly recommended that a qualitative phase of research is initially conducted, the main purpose being to understand the vocabulary and language used by the customers as well as understanding their motivations and attitudes towards given services, products and usage occasions. The findings of the qualitative research provide invaluable input to the quantitative stage in terms of the line and tone of questioning, and of course the overall structure and content of the quantitative phase. (ABMRC, 1989, p.26)”

In addition, it is worth underlining that the data was collected from seven different units of the case company. This combination provides a more accurate view of the research topic and adds objectivity to it.

While response rate alone does not represent the quality of a study, it is one indicator that editors of academic journals use in determining the potential contribution of a study (Campion, 1993). Baruch and Holtom (2008) carried out an extensive study related to the research response rates, in which they analysed 490 organizational research articles published in 17 different academic journals in years 2000 and 2005. The results of their study show that surveys used in these articles had an average response rate of 52.6 percent in the studies published in 2000, and 52.7 for the studies published in 2005, both with a standard deviation of circa 20.
The surveys conducted via e-mail (in this research we have used an online tool with link sent automatically by the system via e-mail) had the average response rate of 54.7, with the standard deviation of 23.9. It is interesting to note that many articles were published in academic journals without providing the response rate of the data collection. Baruch & Holtom (2008) suggest that a response rate that exceeds the boundaries of one standard deviation should be discussed. Thus, the achieved response rate of 96% can be considered to be fully in line with the quality standards of academic organizational research.

6.4 Limitations of the study

As for every research, this study has also limitations. First, this research was conducted as a case study for a single project, developing the IT risk assessment framework of a single case company. Therefore, the results are limited to the context of the organization in which they were studied, and are not directly applicable to a wider organizational context.

Second, IT risk management, and IT risk assessment in particular, despite having a vast literature in its support, it is a constantly developing subject particularly in the light of the most recent technological advancements (Amer, 2011). Therefore, any approaches taken and comments given during the conduction of this study may become outdated quickly as the field is studied further and new theories and approaches are discovered.

Third, the author is familiar with the case company due to his job and position as an IT cycle owner and decision maker. Thus, the author was familiar with all but one of the interviewees. The existing role of the author, and the internal professional relationships could have an effect on the interviews and consequently on the information provided in the final research paper.

6.5 Next steps

The present research provided results that were above the defined targets settled by the key stakeholders. Furthermore, top management expressed clearly its satisfaction with the newly defined IT risk assessment process framework and current maturity level. There is currently no indication that the case company would need an higher level of maturity in IT risk assessment.

At the same time, the work performed purposely concentrated, as said, only into the IT risk assessment. This, there are other opportunities to improve IT risk management cycle in the case company.

In particular, three additional specific areas to be developed under IT risk management have been identified during the last iteration of Gartner maturity survey. At the moment, due to specific internal reasons related to the challenges that the case company will need to face in 2016, no additional process improvement have been agreed in IT risk management cycle.

Anyway, a roadmap for 2017 & 2018 have been developed, with the following high level

actions that represents the next steps in relation to IT risk management development (see Table 9).

Table 9: Next steps in IT risk management cycle development in the case company.

Timing	Main Activity	Outcome
Q4 2016	Review with selected top management members the potential development areas in IT risk management identified during the second iteration of Gartner survey.	Feedback on how to proceed in relation to the development of this area.
Q1 2017	Based on the feedback received, preparation of the project plan, which is going to be presented to key decision makers for feedback and approval.	Project plan defined and approved.
Q2 2017	Once the project is approved, budget will need go through the review of dedicated investment bodies.	Budget for the project is granted.
Q3 2017 – Q3 2018	Project is executed according to plan	Project goals are hopefully reached.

6.6 Suggestion for further research

Even though this study has specific limitations, as explained in this chapter, I have been thinking about how this work could be useful as starting point for future research, reaching two suggestions.

First of all, a similar study could be conducted in multiple companies to see what kinds of variations exists between organizations in terms of how to manage IT risk assessment. This analysis would provide a practical point of view that is missing in the current framework and literature, helping IT risk managers to select the right IT risk assessment approach for their organizations.

Secondly, in this research we have not examined the challenges faced in the process of implementation of the IT risk assessment framework in the case company. It would extremely interesting to conduct a research on the issues faced by several organizations during the implementation of IT risk assessment and on how this issues have been managed. In this way, a new research could support the improvement of IT risk assessment implementation in companies, aiding IT risk practitioners to avoid or solve efficiently the same challenges faced by other organizations.

References

Alasuutari, P.; Bickma, L.; Brannen J. (2008): “The SAGE Handbook of Social Research Methods”. SAGE Publications Ltd.

Ames, B.; Brown, F. (2011): “Auditing the cloud”. Internal Auditor. Aug2011, Vol. 68 Issue 4, p35-39.

Astromskis, S.; Janes, A.; Sillitti, A.; Succi, G. (2014): ”Continuous CMMI Assessment Using Non-Invasive Measurement and Process Mining”. International Journal of Software Engineering & Knowledge Engineering. Nov2014, Vol. 24 Issue 9, p1255-1272.

Baruch, Y.; Holtom, B.C. (2008): “Survey response rate levels and trends in organizational research”. Human Relations, 61(8), 1139-1160.

Brewer, J.; Hunter, A. (1989): “Multimethod research: a synthesis of styles”. Newbury Park. Sage.

Cain, A. (2013): “Prepared for a data breach?”. Internal Auditor. Jun2013, Vol. 70 Issue 3, p13-13.

Campion, M.A. (1993): “Article review checklist: A criterion checklist for reviewing research articles in applied psychology”. Personnel Psychology, 46, 705-718.

Ebert, C. (2004): “Getting Started with the CMMI”. IEEE Software. Jul/Aug2004, Vol. 21 Issue 4, p92-94.

Gerring, J. (2007): “Case study research. Principles and practices”. Cambridge University Press, NY.

George, A.L.; Bennett, A. (2005): “Case studies and theory development”. Cambridge, MA: MIT Press.

Glesne, C.; Peshkin, A. (1992): “Becoming qualitative researchers. An introduction”. Longman, NY.

Guba, E.G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. Educational Communication and Technology, 29, 75-91.

Iliescu, F.: “Auditing IT Governance”. Informatica Economica. 2010, Vol. 14 Issue 1, p93-102.

International Organization for Standardization (ISO) (2009): “IEC 31010: 2009 Risk management – risk assessment techniques”, 2009.

International Organization for Standardization (ISO) (2009): “IEC 31000: 2009 Risk management -- Principles and guidelines”, 2009.

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) (2008): “ISO/IEC 27005: 2008: Information technology – security techniques – information security risk management”. 2008.

Joseph, J. (2013): “How safe is your private information?”. Isaca Journal. Mar.2013, Vol. 2, pp.16-20.

Kent , Anderson (2007): “Convergence: A holistic approach to risk management” Network Security. May2007, Vol. 2007 Issue 5, p4-7.

Kissel, R.; Stine, K.; Scholl, M.; Rossman, H.; Fahlsing, J.; Gulick, J. (2008): “NIST special publication 800-64 revision 2: system considertions in the system development lifecycle’. National Institute of Standards and Technology (NIST).

Kouns, J.; Minoli, D. (2010): “Information Technology Risk Management in Enterprise Environments”. ISACA publications.

Fenton, N.; Neil, M. (2012): “Risk Assessment and Decision Analysis with Bayesian Networks”. ISACA publications.

Gartner (2014, 2015): “ITScore Overview”. Gartner Website.

ISACA (2009): “The IT risk practitioner guide”. ISACA. 2009.

Lainhart, J. (2000): “COBIT™: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities”. Journal of Information Systems: Supp., Vol. 14, No. s-1, pp. 21-25.

Marsland, N.; Wilson, I.; Abeyasekera, S.; Kleih, U. (1998): “A methodological framework for combining quantitative and qualitative survey methods”. Background paper – types of combinations. Report written for DFID Research project R7033.

Marsland, N.; Wilson, I.; Abeyasekera, S.; Kleih, U. (2000): “A methodological framework for combining quantitative and qualitative survey methods”. Socio-Economic Methodologies for Natural Resources Research – Best Practice Guidelines (NRI and DFID).

McCollum, T. (2013): “Regulations Top IT Audit Concerns“. Internal Auditor. Jun2011, Vol. 68 Issue 3, p14-15.

Nico, M; Fakhry, H (2013): “Using COBIT 5 for data breach prevention”. Isaca Journal. Sept.2013, Vol. 5, pp.23-29.

Parthajit, P.: “The OCTAVE approach to information security risk assessment”. Isaca Journal. July 2009. Volume 4.

Ramamoorti, S.; Sridhar, N. (2013): “The importance of information integrity”. Internal Auditor. Feb2013, Vol. 70 Issue 1, p29-31.

Reding, K. & Others (2013): “Internal Auditing: Assurance & Advisory Services, Third Edition”. The Institute of Internal Auditors.

Ritchie, J.; Lewis J. (2003): “Qualitative research practice: a guide for social science students and researchers”. SAGE Publications Ltd.

Ross, S. (2013): “Information Security Matters: Emo, Ergo Sum”. Isaca Journal. Oct.2013, Vol. 5, pp.4-6.

Ross, S. (2013): “Information Security Matters: Mean times”. Isaca Journal. Jan.2013, Vol. 1, pp.5.

Shanahan, M.(2011): “Introducing the New COBIT Assessment Programme: Why and How It Is Replacing the COBIT Maturity Model”. COBIT Focus. Vol. 4, p5-9.

Shenton, A.K. (2004): “Strategies for ensuring trustworthiness in qualitative research projects”. Education for Information, 22, 63-75.

Steuperaert, D. (2009): “Identify, Govern and Manage IT Risk”. COBIT Focus. 2009, Vol. 4, p15-17.

Steuperaert, D. (2010): “Using the Newest ISACA Framework, Risk IT”. COBIT Focus. 2010, Vol. 1, p3-4.

Yu, W. (2013): “A COBIT approach to regulatory compliance and defensible disposal”. Isaca Journal. Sept.2013, Vol. 5, pp.31-33.

Wlosinski, L. (2013): “IT security responsibilities change when moving in the cloud”. Isaca Journal. May.2013, Vol. 3, pp 34-38.

Title of the Appendix

Content of the appendix is placed here.

Title of the Appendix

Content of the appendix is placed here.