UNIVERSITY OF GOTHENBURG

Integrated project risk management in program context

Master of Science Thesis in the Masters Degree Programme
Software Engineering and Management

VARD ANTINYAN
SPYRIDON MANIOTIS

University of Gothenburg
Chalmers University of Technology
Department of Computer Science and Engineering
Göteborg, Sweden, June 2012

Integrated project risk management in program context
A complete stepwise risk management approach for financial IT programs

VARD ANTINYAN
SPYRIDON MANIOTIS

Examiner: CHRISTIAN BERGER

University of Gothenburg
Chalmers University of Technology
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

[Cover:
Schrodinger's cat is a thought experiment cat that might be alive or dead, depending on an earlier random event. http://emi4art.com/cats.html.

Department of Computer Science and Engineering
Göteborg, Sweden June 201212

Acknowledgement

We would like to show our appreciation and gratitude to all those that have been involved in the whole process of this thesis. Therefore we would like to thank:

The Head of Design and Deployment of M-Commerce of Ericsson, Herwig Stöckl for giving us the opportunity to work on this topic and for the provided information and input,

The owner of Lichtenberg & Partners Professor Steen Lichtenberg for his valuable feedback and guidance on the creation of the perceptive method,

The Head of Software Engineering division of Chalmers University of Technology, Professor Jörgen Hansson for offering his valuable time and helping us to write this report,

Professor Joakim Jahlmar from the department of Languages and Literature at the University of Gothenburg for his valuable help regarding linguistic aspects of our work

Gothenburg, May 2012

Vard Antinyan
Spyridon Maniotis

Abstract

Ericsson Money Services as a financial software program develops mobile services the aim of which is to provide worldwide money transactions. The development of the service includes multifunctional processes and a number of partnering organizations hence emerging hindrances in uncertainty management and risk assessment. On the one hand the vast influence of the external factors on the program and on the other hand the multiple projects running under the same program hamper to apply the traditional risk management approaches effectively. Financial programs encompass variety of dynamic processes and the risk management process becomes a momentous activity to be done thoroughly. This thesis work examines the main issues of traditional risk management methods while applying in financial software development processes at the same time provides a stepwise procedure to guide what information must be collected and registered, how the evaluation processes must be carried out and what approaches to apply in order to succeed in the risk management activities in program level. The information that we provide on how to register the potential hazardous events is not optional for any financial software program as it can be specific dependent on external influencing factors. Conversely the estimation methods are all-embracing and do not require further examination in its application in other software programs. The specified eight plus one steps of risk management iteration herein framework provides a complete guide on how to carry out the risk management activity without other supportive guidance and additional advanced knowledge in the field. The examples we cite in the thesis are chosen both concerning to the field and simple life situations to be easily graspable. The risk-specific information that must be registered is discussed and guided. In addition the procedure that we present and the information that must be collected specifically for Ericsson Money Services operation are implemented and provided in the tool of UniRisk.

List of Figures

List of Tables

Table of Contents

This page is intentionally left blank

1. Introduction

But indeed, another way is open to us here by which we may obtain what is sought; and what you cannot deduce a priori, you can at least deduce a posteriori.
Jacob Bernoulli, 1713, in his "Art of Conjecture"

Any type of organization irrespective what the field of its performance is, has to make optimal decisions while carrying on business operations. The decision making is a core action towards reaching any kind of goal. Whenever the appropriate decision is made it becomes clear which the following actions are. But how optimal our chosen decision is can be checked later on when we have results. Before the final results we have only uncertainties. Does not matter what the source of the uncertainties is and why it can have malicious consequence we need to have an idea of how to measure the possible impact of it on our life or goals. Although we are sometimes unable to prevent the possible adverse event on us or our properties, we are always capable to measure its likelihood and severeness and thus frame several strategies to avoid or reduce the effect of it. But there is always a variety of factors that becomes hindrance while measuring the probability of adverse events and sometimes even the impact. In the field of software engineering a widespread measurement method is the traditional risk assessment method which implies to measure the probability of the adverse event, the impact in case the event happens and calculate the product of that two values which is usually called risk exposure and shows how much the average loss is [10]. Another mainstream is the three point estimation method which implies that the expected impact of loss is uncertain and suggests establishing the upper and lower bounds of the loss [9].

In the field of software engineering when a multifunctional and hierarchical program runs towards a set of goals and contains several projects, the effective risk management becomes a complicated task. The main reason is that not only the assessment and mitigation of risks are important activities but also the understanding of how the same risk can affect different projects and how these projects are interconnected each other because of common adverse event. The multiple mitigation activities because of the same risk take a lot of unnecessary cost, so the communication between these projects becomes a vital activity. Also different projects apply different software development methodologies thus they require different frequency of risk identification and mitigation sessions. Because of unparallel risk management activities the communication usually can fail among different projects and unnecessary expended cost for a risk is inevitable.

Ericsson Money Services as a financial program which contains several interrelated projects is a typical example of the upper described software program. An effective and easy-to-use program risk management method, which unifies such important activities as identification, analysis, mitigation, control and monitor, dependencies of several projects due to the same hazardous

situation and other minor activities, is one of the success factors to measure and keep track of opportunities and risks.

In this thesis work we introduce a software program risk management approach which can be applied for any kind of software project development processes integrated within any development methodology. Additionally we propose a new technique of risk assessment which combines quantitative and qualitative assessments of risks. We also discuss the downsides of the traditional and triple estimation methods, where those two are effective to apply, how to avoid erroneous results and how to bypass the emerged problems while assessing the risks.

1.1. Definitions and Abbreviations

EMS (Ericsson Money Services)	Mobile money service launched by Ericsson
HUB	A wired network that connects different devices together
MiniRisk	The checklist tool used by Ericsson for the purposes of risk management
UniRisk	The risk management checklist tool as the result of the thesis
SDP (Solution Design Program)	The program of Ericsson under which Ericsson Money Services run
YEN	The official currency of Japan
GBP	The official currency of the United Kingdom
EURO	The official currency of the Euro zone countries
SEK	The official currency of Sweden
KPI (Key Performance Indicators)	Performance measurement indicator

Table 1: Definitions and Abbreviations

1.2. Thesis disposition

The thesis is divided in three main parts. The first part consists of sections one and two starting with an introduction to the studied field, an overview of the field's background and a detailed presentation of the Ericsson Money Services operation. Continuing in this part we describe the problem domain, analyze the purpose of the thesis by defining specific research questions and present the results of our work along with the followed working methodology. The second part is the core part of the presented document through section three and provides our approach of solving the problem domain points. Our solution is broken down into sequential steps in order to provide the reader with a comprehensive and complete understanding. We start each section of

this part by providing the background and theory of each step. We continue by outlining our concerns, issues and points to be improved along with a simple scenario in order to describe how the theoretical background is connected and applied to real world situations. The third and last part consists of sections four, five and six and provides the evaluation of our work, points of discussion and further research concerns. Concluding the document we draw our conclusion based on our findings and experience of doing this thesis.

1.3. Background

"Those who cannot remember the past are condemned to repeat it."
Socrates

Life is full of uncertainties that can have negative or positive impact to our actions and plans. Some of these uncertainties can be measured and some not. Whenever the uncertainty is measurable it means we can measure the probability of the uncertainty and the consequences of it on our environment. When the uncertainty is related to human life, activities or goals we are used to say that there is a risk or risky situation. A risk for an individual or an organization is a possibility of an adverse event to occur and have impact to their properties, reputation, goals and/or objectives. Conversely an opportunity is the possibility of a favourable event to occur or not and have impact to properties, reputation, goals and/or objectives. In reality we use to keep track more of risks than of opportunities because the security of what we already have is more important than the hope to get things without earning. A positive property of risks is that we can prevent and eliminate them by performing some activities related to the management of them. The related activities in order to manage risks are organized and applied through risk management. The risk management process is used when we want to quantify and qualify potential risky situations that might bring potential losses to current or future investments.

Risk management nowadays becomes more and more popular in the field of software engineering and applied IT, although it is in an immature level in contradiction with the financial and insurance domains. But different domains have different concerns and therefore different risks and approaches to risk management [15][19]. For instance a project manager responsible for a mobile application game has concerns of attractiveness of the game and can identify risks relating to it. On the other hand a failed money transaction through a banking system is conceptually different risk that might cause loss of money and definitely damage the reputation of the bank and the trust of the customer.

The importance of risk management in software engineering and applied IT is driven through different factors. The most important factor is the number of failed projects that have impact to the financial stability of the organizations and to the overall reputation of the organization as well [7]. A failed project can express high unmanaged cost to the organization by influencing the

financing of other projects that are related to it and also by influencing the financial state of the organization. There are many examples of organizations that have failed to apply risk management and the financial collapse of a project led the organization to bankruptcy.

The most common and effective way to deal with risk management process is to apply it and integrate it within the project management methodologies. The parallel and systematic application of them to a project minimizes significantly the chance of a project failure or exceeds the initial financial plan. Unfortunately there is no any formal existing methodology to combine both risk and project management and the application of both depends on the organization, the industrial domain that the organization operates in, the project type and the project management methodology that is applied. Thus risk management is a very flexible process that might consists of fixed steps as we see in the coming sections of the thesis but nevertheless these steps can be adjusted, modified and applied with respect to the nature of each project and standards that different organizations apply.

1.4. Ericsson Money Services

"In an age where a single click books a flight or updates your relationship status, isn't it a bit strange that your money is still so … analogue?"
Ericsson, EMS (2011)

Since August 2011 Ericsson launched its first of a variety of new mobile money services which is called Ericsson Money Services. Ericsson Money Services was initially launched and operates in seven European countries which are Sweden, UK, France, Germany, Italy, Spain and Poland. This was the first step by Ericsson in order to expand the service availability to the rest of Europe and also in a word wide range and become a global service in the future. Through Ericsson Money Services Ericsson aims to provide a full suite of convenient, cost-efficient, secure and instant mobile financial service to consumers globally. Users can sign up and create easily a safe and secure online mobile wallet. They are able to access their money safely from the Ericsson Money Services network through their mobile phones in order to send, receive money from and withdraw cash. All the transactions described above are done through a network that connects the electronic money wallets with different telecom operators and banks across the world.

The whole process of money transaction via Ericsson Money Services is done with a simple SMS message. The user can send a simple text from wherever he/she is located to another person who sits in the next corner or to a relative who lives thousand miles away. The service offers greater freedom of choice, access to money and a faster and more convenient way to transfer money to friends and family. People who can use the service are:

- Families: parents can send money to their children that are away at the university, on holidays or in a gap year.

- Social sharers: people can conveniently share the cost of a meal, settle small debts and transfer money between friends and family.
- Cash-only consumers: consumers used to transacting only with cash can take a first step into banking.
- Non-domestic workers: overseas workers can send money back home to their families without having to use postal or personal cash transfers, which are often time-intensive.

Using a simple scenario we describe a possible money transaction using Ericsson Money Services in order to provide the reader with an outline of the service operation. Suppose that Ida, who lives in Sweden wants to send some money to her friend Jane, who lives in UK and once again she wasted some of the money that she is supposed to pay her rent with. Both the two friends have completed the registration process to the service and they have provided the required information in order to complete the secure process, using their mobile phones. After, Ida wanted to fill her account on her mobile wallet by providing her credit or debit card and her bank account or even cash. Eventually she loaded 1000 SEK from her bank account to her mobile wallet. Then she wanted to send the 1000 SEK to her friend Jane. Instead of waiting around three days for the transaction via a banking system, she performed a few clicks on her mobile phone and the money was instantly transferred to Jane's money wallet together with an SMS confirmation. The figure below visualizes the money transaction from mobile wallet – to – mobile wallet using the blue dotted line. The red dotted line symbolizes the time latency of the traditional money transaction through a common bank – to – bank account which is significantly slower.

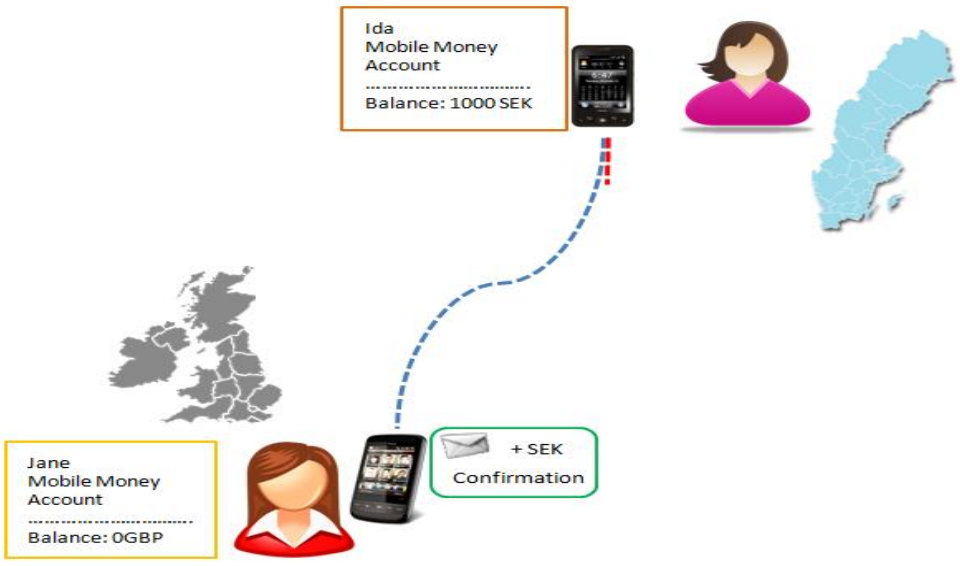

Figure 1: Simple mobile-to mobile money transaction through Ericsson Money Services

The transaction was done through a sequence of steps performed by Ericsson Money Services. When Ida pushed the "send" button on her mobile phone a series of events were sent to the Ericsson service provider of Sweden that got the transaction. After the service provider of Sweden forwarded the transaction to the central interconnect HUB of Ericsson Money Services. The central HUB converted the currency and sent the transaction to the service provider in UK. The UK service provider performed all the debit and credit transaction at the same time and afterwards it sent the transaction to Jane's mobile wallet. All the transactions described above are visualized in the figure below.

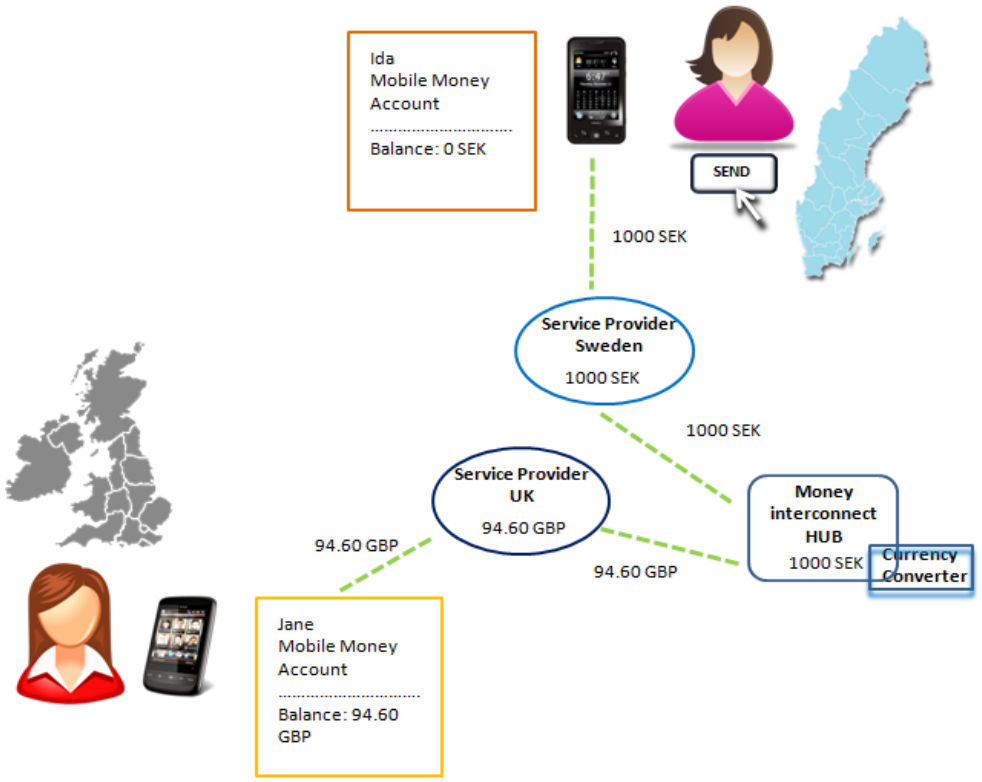

Figure 2: Basic interactions between devices though Ericsson Money Services operation

As Ericsson claims, "Ericsson Money Service is a money transaction from point A to point B which is fast, simple and in the hand of the user [20][21].

The operation of Ericsson Money Services seems to be simple, but in reality lurks many critical concerns and potential risks. In order for the service to run successfully these risks have to be identified and dealt with. Ericsson applies risk management aiming to eliminate the potential risks, but is the common risk management approach for a typical IT project applicable to a financial IT project as Ericsson Money Service? If it is not, how can we make project risk management efficient for financial IT projects? The answers to these questions we find out in the coming sections of this framework.

1.5. Problem Domain

"We cannot solve problems by using the same kind of thinking we used when we created them."
Albert Einstein

The problem domain of this study was initially provided to us by the Head of Design and Deployment of Ericsson. Ericsson Money Services is a new business area for Ericsson as it is their first financial IT project. Even if it applies the same or a similar risk management approach within this area (IT projects), there are some new and undiscovered risks that possibly will occur. The global character of Ericsson Money Service and the assignment of new sales teams frequently contain these new undiscovered risks. In order to minimize the risk to not capture the most important and regular seen risks, a kind of intelligent risk checklist for financial IT projects needs to be developed.

Based on the strategy and the uptake of new contracts there were a variety of solutions and process development activities ongoing within Ericsson Money Services organization. Those activities were summarized in a program called Solution Design Program. This program contains several projects, in which different project development methodologies such as Agile and Waterfall are applied. The Waterfall model based projects follow the PROPS [17] methodology, whereas the Agile projects run according to Scrum [2]. The Solution Design Program is also heavily connected to the program that drives all customer projects since most of the customer projects are dependent on deliveries of it. Neither the size of the Solution Design Program, nor the volatility in the activities are on a level ensured that an application of a full-scale risk management suits.

In addition it has been identified that the program, its projects and subprograms need to keep track of risks and opportunities as well as of dependencies among projects due to emerged uncertainty factors across the projects. The terminology of dependencies particularly refers on the one hand to the dependency of risks that exist in different projects running under the same program and on the other hand to the dependencies of projects due to common risks. This is how common risks influence the operation of specific projects on the one hand and the whole program on the other hand. Simply stated, *a risk dependency concept in a program is the interrelation of two or more projects due to an emerged risk in any of those projects.*

Simplifying the description above, we have derived two main points of the problem domain that are presented below.

- MiniRisk does not foreseen for international financial IT projects. An international financial IT project is a long-term industrial project, based upon the projected cash flows, across different systems and devices that cooperate for the accomplishment of the goal determined by the project.

- There is no standard method to keep track of opportunities and dependencies among projects that run under the same program in order to achieve a greater goal.

As it is described above, the problem domain seems to be general without referrals on specific malfunctions and drawbacks of MiniRisk. The examination of the MiniRisk has disclosed the omissions and downsides that we present below.

- When it comes to financial IT projects the source of the risk can be heavily depended on external factors, such as to which country the customer belongs to, with whom the organization has a contract and what type of customer it is (financial institution, organization, etc). Governmental, legal, and constitutional rules differ from country to country and from organization to organization creating variety of issues. The spawning uncertainties at this range are wide and need to be sorted and classified.

- Whenever a risk is identified we may have principally different mitigation approaches or strategies. Every such strategy has a cost and the potential for risk reduction. The issue is that there is no unequivocal index for cost-effectiveness to indicate which mitigation approach is the best one to be applied. Mostly the experienced risk managers can judge from loss distribution parameters and specific tasks which strategy would be the optimal but when those parameters are getting to a similar range it becomes a tricky task.

- The current applied method that is based on the three point estimation technique [22] has some inefficiency due to undefined type of loss distribution, skewness effect of the distribution and such called "either-or" type of risks, which are events that might turn up and if they turn up there is a severe effect.

- Another issue appears when the risk management process contains some uncertainty factors and the parameters of these factors might vary over time. The reasons of these variations can be different. The severity of impact, the likelihood of adverse event, how much it concerns to the specific task and how widely it can affect the other projects, as well as on the overall organizational assets can also vary. The absence of control to the upper mentioned issues may bring some serious problems. Based on such problems, risk management must capture not only the phases of identification, analysis and mitigation but also the control on its evolution simultaneously.

- While performing risk management in projects the whole process is relatively more efficient. When it comes to program level, having different interconnected projects running towards the same goal, the risk management process becomes a complicated and competitive task. One reason is that risks which emerge in one project can somehow affect other projects and the program as a whole. Another important reason is that one risk emerged in one project can be heavily correlated to another risk in a second project. Sometimes even risks are counted twice or several times on different projects or even

worse, not counted at all because it is expected to be counted in one of the other projects. Those factors can create an impediment towards effective risk management.

The purpose of the thesis and the outcomes is discussed in the coming section.

1.6. Purpose

"Efforts and courage are not enough without purpose and direction."
John F. Kennedy

The purpose of this study is to provide solution for managing risks in financial IT projects in program context. We aim to provide guidance for all the phases of the risk management iteration and to meet the needs of both experts and beginners in the field. Also we intend to provide suggestions on how to use risk management iterations in the most productive way and an accurate outcome along with a new approach of how to perform some specific steps on the iterations. Below we list the concerns as we have received them by Ericsson.

- Create intelligent risk checklist tool for financial IT projects such as Ericsson Money Services.
- Differentiate between different types of contracts, different types of legislations in the target countries and different kinds of partners (telecom operators, banks, etc.).
- Use the Solution Design Program (SDP) characteristics and information which already applies two different project development processes such as Waterfall (PROPS model) and Agile (Scrum methodology) to analyze and define a new approach.
- Create a new risk management approach for SDP risk management operation in order to allocate risks among projects applying different project development methodology.

In order to be able to achieve the purpose described above and at the same time successfully fulfil our thesis, we derive the following research questions placed bellow.

RQ1: How could we frame an easy and efficient approach of software project risk management, that is applicable within the Solution Design Program and within any project that apply the same development methodologies (PROPS or Scrum) as the Solution Design Program projects?

RQ2: Could the new software project risk management approach be integrated and applied on software development processes?

RQ3: How to frame an effective and easy-to-use method to deal with risk dependencies and how can it be integrated with the software project risk management iteration and the new checklist?

1.7. Results

"I've always believed that if you put in the work, the results will come."
Michael Jordan

The analysis of available data and the problem statement implies the general expected outcome of this work as it is presented bellow with bullet points:

- An efficient way to work with the risks of financial IT projects. It should differentiate between different types of contracts, different types of legislation in the target country and different kind of partners (Telecom operators, banks, etc.).
- Creation of a simple, efficient, transparent and easy-to-understand-and-maintain risk management instrument, in order to carry out an efficient risk management process. Efficiency in this case is quite high standard, as industry standards in financial IT projects are significantly high.
- Examination of both the empirical analysis and theoretical background of risk management and the adaption of the new approach to both areas.
- The allowance of an easy-to-be-followed, able-to-be-integrated in the risk management iterations and understandable through simple steps risks dependencies controlling method.
- A concrete and thorough final paper to communicate our findings and the final result of our work. This paper should be easy to be read and understood, by people from the industry like the Head of Design and Deployment of Ericsson, people in the research area, like our university supervisor and people who have only slight relation with the domain of risk management, like our university colleagues.

2. Methodology

"Method is much, technique is much, but inspiration is even more"
Benjamin Cardozo

This section focuses on the research and working methodology that we have followed in order to finalize this thesis. The purpose of this section is to provide an overview of all the activities that have been carried out during the life cycle of our work. We have started with our project plan and the work break down structure along with the strategy that we followed in order keep track of time and activities and also to deliver specific tasks. In addition, we provide the resources collection, analysis and validation, concluding with a reference to our communication plan.

Planning

At the earliest phase of our work, in collaboration with our Ericsson supervisor we created a concrete and flexible project plan which would be our compass, guidance and common understanding of what to deliver and when. In the project plan we have also specified the internal and external interfaces of our project organization. The internal team organization interfaces includes the two of us as master's students at the IT University of Gothenburg doing their thesis, on the topic of "Integrated project risk management in program context". On the other hand the external organizations were Herwig Stöckl as our Ericsson supervisor, Jörgen Hansson as the university supervisor and every other stakeholder who contributes to our work. Having the stakeholders identified, we assigned the key roles that everyone would have during the thesis.

Having the crystallized problem domain, expected outcome, available stakeholders and time constraints clarified we broke down the available time into milestones. In every milestone we have defined the task to be completed, along with the needed input of information and data in order to behold tasks to be examined and completed with the desired outcome. The start date and deadline for each milestone has been also specified. At the end of each milestone the expected outcome has been described. The status and relevant comments in cases of delay, constraints or interesting findings that might influence the rest of the milestones has been reported. We agreed that the project plan should be reviewed and updated every two weeks.

Working strategy

The process we have followed consists of two parts. The first stage of thesis work includes the background, theoretical and empirical study of the domain and the research. The second stage includes the creation of a risk management checklist tool which should operate based on the findings of the first part and be connected to our research study. This second stage represents the implementation part of the thesis.

Our checklist has been created to support the risk management iterations. Therefore we performed intensive research and analysis of the different steps that are followed during the risk management iterations. For instance for the risk identification process, we got a standard iterations steps of how risk identification iteration is being done by our Ericsson supervisor. After we have performed research and analysis ourselves aiming to find vulnerable organizational assets and also see how these assets could be protected. Having the input results of our research available, we have implemented that specific part of the tool that is used for the risks identification. The same process has been carried out for the rest of the tool's functionality. More detailed analysis can be found at the solution section (Section 3) of the document.

Resource Acquisition

The availability, collection, analysis and utilization of resources have been critical during our work and the manipulation of them could make the difference in terms of success or failure of the thesis. The needed information in our case had come iteratively and from a variety of different resources which we present below.

Literature: We have chosen the literature according to our supervisors' guidelines and our own research in the domain. Those included books, research papers and publications. Also we got relevant literature materials that have been recommended by Ericsson.

Standard bodies: Ericsson relies on the Project Management Institute and henceforth follows the ISO 31000 standard of project risk management [22].

Statistical data: We analyzed data that the organization has collected during the life cycle of the Solution Design Program.

Existing solutions: The already existing checklist which is now used for risks analysis and mitigation was given to us. Also we got a detailed description of the Solution Design Program operation, concerning the risks identification and management. In addition we found and we used risk management tools that are available on the market in order to identify glitches on the one hand and get inspiration on the other hand.

Stakeholders: It has been crucial to have stakeholders' clear identification and description. In addition we needed to know the availability of them and the level of involvement that they have in the project. Also we wanted all the relevant information that they could provide to us in order to analyze different tasks.

Resource analysis

Aiming to work in a productive way, we have categorized the needed data in the categories mentioned above. Every single resource, when collected, has been stored according to its usage and context. Afterwards according to the specified task that had to be carried out, we have retrieved the proper data that had to be examined, analyzed and used to contribute our work and increase the level of accuracy and quality. The resource analysis was ongoing during the whole life cycle of the thesis project.

Resource credibility

Having many resources collected almost every day, it was of great need to check the credibility and objectivity of them. We have examined specifically the source of information and the time period during which they were being available. Some of the collected resources has been decided to be unnecessary or inaccurate and therefore they had to be removed without further usage. Knowing that the resources provided by Ericsson and the books written by the experts in the field of risk management are credible enough, we had to focus our credibility research on the on line resources and the research papers particularly. Therefore we analyzed in depth the results that the related books and research papers were bringing to the light. By combining those results we judged which really interesting findings were and therefore they could be used as support to our work and which were inaccurate and could bring misunderstandings and wrong assumptions.

3. Proposed Solution

"When you think you can or you cannot do something, you are probably right"
Henry Ford

In this section we provide a stepwise procedure describing how to identify, assess, mitigate, control and communicate the arisen risks. The first eight steps are in full description of financial IT project risk management and the ninth step is the guidance of how to communicate the common risks in interconnected projects in a program context.

3.1. Project Risk Management Iteration

"Be prepared to cut your losses - Cancelling bad projects early is success because you save time, money and resources that can be applied to better opportunities."
Kurt Bittner, "Managing Iterative Software Development Projects"

As *project risk management iteration* we consider all the necessary activities that are performed through the entire life cycle of a project in order to identify, evaluate and eliminate potential risks partly or completely. It is described as a continuous sequence of phases and the completion of them aims the successful handling and confrontation of risks. The project risk management iteration is an ongoing activity that is applied within the project development methodologies. It starts with the requirements specification and continues till the project's deployment and maintenance. The business and systems goals are analyzed with respect to uncertainties and threats that can influence our decisions. During the phase of project risk management iteration is the first time that most of the project stakeholders sit at the same table and perform business and systems analysis with respect to uncertainties.

According to the Project Management Institute [18], the phases of project risk management are six. Our approach includes the existing defined phases plus two additional phases due to the special character that financial IT projects have. Therefore a complete project risk management iteration for financial IT projects according to our research should consists of eight phases where each one has a specific expected outcome and an optional ninth one in case of correlated projects in program context. These eight plus one phases along with their expected outcome are presented below.

Risk management iteration planning: A specific approach and plan for project risk management is defined. The frequency of the iteration, the facilitator and key participants of the project risk management iteration are specified also.

Risk identification: The risk management team identifies the potential adverse events and makes decisions which of them are severe enough to be examined further. The outcome of this phase is a full list of potential risks and opportunities that might have positive or negative impact to the project.

Risk qualitative assessment: The risks that we have identified in the identification phase are evaluated qualitatively. The relative probability of a risk to occur and the relative effect are calculated along with the evaluation of exposure.

Risk quantitative assessment: The risks are assessed in terms of money. The effect that the risks have on the overall project objectives and assets is analyzed with respect to the time plan and budget of the project.

Risk response plan: The response in order to deal with each risk individually is specified. During this phase all the available options and actions are defined in order to enhance opportunities and reduce threats to the project objectives. After this phase every risk has its corresponding response plan.

Risk analysis: The analysis of the different available responses to a particular risk is performed. The cost of the response plan to the overall project budget is examined and the optimal countermeasure is chosen according to its cost-effectiveness.

Risk monitor and control: The uncertain events that influence a risk and the performance of the response plan are tracked. In addition the effectiveness of the response plan is evaluated throughout the project life cycle.

Analysis of inceptive event of risk: Inceptive hazardous events that might become potential risks of the project are identified and monitored.

Risk iteration report: A complete report containing all the relevant information about the results of the project risk management iteration is handed to the project or program manager and to the project stakeholders for evaluation and confirmation.

Risk dependencies management: This phase is applied to correlated projects that run under the same program. After the completion of each project risk management iteration for each project individually, a coordination of actions between the different projects takes place in order to report correlated risks and dependencies of risks among the different projects.

The frequency and number of project risk management iterations depends on the character of each project and can vary from organization to organization. The three most important factors that determine the frequency of the project risk management iteration are the software development methodology that is applied to a specific project, the longevity of each project and the variability of factors that influence the project. As it has been reported to us by Ericsson the project risk management iterations differ in terms of frequency among projects that have high longevity and projects that have low longevity. In projects that have high longevity the project risk management iteration is performed only once at the beginning of the project, and on the contrary, projects that have short longevity are exposed to project risks management iteration every two weeks. Also projects that apply Agile Scrum are more likely to apply project risk management iteration more frequently than projects that apply the Waterfall PROPS.

In our case as, we deal with a financial IT project, the project risk management iteration is performed very frequently due to the longevity of the project (as Ericsson launches runs and maintains Ericsson Money Services). Project longevity implies many uncertain technical and financial factors that influence the project and the variety of different partners that co-operate towards the goal of the service. In the following sections we focus on every phase of the project risk management iteration individually and provide our approach on how project risk management should be applied to financial IT projects.

3.2. Risk Identification

"I recently realized that I have wasted all my life trying to identify risks and opportunities."
Anonymous

The first phase of risk management iteration process is the identification of adverse events which can affect our business operations, resources, information, reputation and any kind of organizational assets (In this section we do not describe the ways and techniques how to identify hazardous event as this task is not addressed in this framework). Every organization has its own way to identify risks and opportunities. Instead we show what information must be registered along with risk description to make the whole process easily manageable. In financial IT projects, not only issues concerning requirements engineering and maintenance request but also

direct business operations with partners can originate variety of risky situation. We discuss Ericsson Money Services operation as a financial service and some examples concerning it to clarify the risk identification phase for the reader comprehensively.

Dependent on what kind of business activities the organization carries on and who the business partners are we need to register some standard categories of risk generating environments or initiator factors. Ericsson Money Services provides so called mobile wallets for its user to transfer their money from one country to another or from place to place by using their mobile device. For instance if John wants to transfer money from UK to his friend Kate who lives in Japan, he can use his mobile to send money to Kate's account. Kate can see on her mobile the notification that John has sent the money. To realize this operation Ericsson Money Services needs to have business partners in both UK and Japan. Usually money transferring operation in any country can be done by financial institutions such as banking systems. As the service relies on mobile functions Ericsson needs to have telecom operators as partner also. The transferring process can be done then by connecting Ericsson's central transferring system (Ericsson money interconnect hub) to local transferring systems of both countries UK and Japan. The banking systems and telecom operators who are partnering with Ericsson together are responsible for John's money to be reached to Kate. In this context we can outline generally all the issues, problems and agreements that can emerge in this process. For instance the exchange rate variation of currencies between Japanese YEN and UK GBP can spontaneously imply a question: Who are responsible for this risk? This becomes a matter of agreement between partners. Another example can be: Are there any legal issues in these countries while performing money transaction? It could be, as legal restrictions on organizations are actual.

In order to provide a better overview of this phase we identify two potential risks that we use also as guidance for the coming phases of the risks management iteration.

Suppose we have such risks:

Risk1: Chance of failure of the money transaction between the main Ericsson money interconnect HUB and two local service providers of UK and Japan.

Risk2: Exchange rate variation between YEN and GBP can cause loss of profit for Ericsson.

The first risk concerns to service providing function reliability which can be weaken because of different issues of solution design. If the transaction process fails (John fails to send the money to Kate because of system failure) one of the partners is responsible for it. Dependent on what the cause of the failure is and the established agreement the responsible for it could be Ericsson, the service provider or a partnering company in Japan or UK.

The second risk, exchange rate variation, endangers the profit of one of the partners. Again according to agreement one of them must be responsible for the unpleasant situation. Of course while framing risk analysis method for financial IT projects we cannot analyze all the possible

adverse events deeply and in detail, because it is effective to identify and mitigate every special case separately, (that is why we have periodical risk management process in the programs or projects) but we can have some general differentiation of sources and categories of hazardous events to simplify the management process and make traceable interdependency between adverse events.

After analysis in the case of Ericsson Money Services we identify the risk differentiating sources which can be categorized as following:

Partner Type:

Dependent on which kind of financial institution or organization the partner is, the activities, roles and emerged issues and risks could be different. In our case we differentiate four types of partners.

- Banking system
- Telecom operator
- Retail merchant
- Other financial institution

The constitutional issues, the vulnerability of activities and other arisen issues can differ from organization to organization and therefore the essence of emerged uncertainties and risks can vary widely.

Standard categories of risks:

- **Solution:** Risks that have to do with the solution, the KPIs, data, requirements, testing and implementation
- **Fulfillment:** Risks that have to do with the service delivery, the acceptance criteria and changes
- **Finance and Accounting:** Billing terms, cost estimations, discount terms, currency and tax implications
- **Security health and environment:** Social and cultural aspects, health, product responsibilities, personal safety and transportation
- **Commercial:** Risks that have to do with the start of the project, the business case, the business model, customers and business critical factors

Financial Operational Sources:

- Exchange rate variation
- Currency depreciation
- Financial crisis
- Legal restrictions on financial organization
- Liability issues between partners

- Unstable financial partner
- Governmental severe changes
- Change or maintenance request

Country: The name of country from where or to where the money are transferred.

For different projects these categories and risks can alter or deepen in terms of efficiency. The main idea behind registering such information is to have generally outlined historical data while dealing with a new partner in a new country. In UniRisk along with all this data we can have a place to register some comments and assumptions about specific risks as we find it could be supportive for the coming contracts or deals. For instance if we identify that in Japan there are some governmental legal restrictions according to which retail merchants cannot perform some specific function fully then we can register this information as a useful data for later other contracts with a Japanese retail company. There could be some specific risks also that would be worth to register. For instance if there is an adverse event that EURO as a currency will depreciate dramatically during the money transaction process, implies that the financial organization will perform a mitigation activity in order not to be affected severely. In this context Ericsson Money Services and the partnering financial institution may come to an agreement on how to share the risks and responsibilities (detail discussion in section Risk Response Planning). This information is worth to keep as a later compass of resolving similar issues arisen with other partnering financial institutions in another country. If we have some beforehand registered information about the later country and financial institution type then we can combine it to depict the hazardous situation more thoroughly.

Using as examples Risk1 and Risk2 that we have identified in the beginning of this section, we register them by providing all the necessary information. It is worth to mention that for the purposes of automation and guidance during the risk identification phase we have listed all the possible choices of source, risk category and partner type that are related to risks of financial IT projects in the corresponding sheet as a dropdown list. Thus the risk identification and registration for Risk1 and Risk2 are:

Risk1:

Description and impact: Chance of failure of the money transaction between the main Ericsson money interconnect HUB and two local service providers of UK and Japan.

Partner Type: Banking System

Category: Financial and Accounting

Source: Unstable financial partner

Country: UK and Japan

Risk2:

Description and impact: Exchange rate variation between YEN and GBP can cause loss of profit for Ericsson.

Partner Type: Banking System

Category: Financial and Accounting

Source: Exchange rate variation

Country: UK and Japan

Having all the risks identified through the identification phase we can now assess and evaluate them aiming to get a clear view of what the likelihood of them to occur is and how much they will influence the project in terms of reliability, performance, financial aspects etc.

3.3. Qualitative Assessment of Risks

"We've done a lot of qualitative research to follow up on those findings. It is a trend that bears out."
Laurie Demeritt

The qualitative assessment of risks is the immediate next phase of the risks identification. During this phase the identified risks are investigated in terms of particular descriptive variables. These variables are, the relative loss which describes the comparative impact that we have in case that the adverse event occurs, the relative probability which refers to the comparative given probability of the adverse event occurrence and the relative exposure which is the product of relative loss and the relative probability describing the comparative exposure of the risk occurrence. Therefore for each risk we estimate the potential relative loss and the relative probability of this risk to occur. Afterwards we multiply these two values and the product of them is the relative exposure that the project has to that risk:

$$Relative\ probability * Relative\ loss = Relative\ exposure \qquad (1)$$

In Ericsson they use a range of three values in order to describe the relative loss and probability. The variables can take the values from 1 to 3, with 1 being the value that describes the least and 3 the value that describes the most. The table below provides a sample of results after a hypothetical qualitative risks assessment for four different risks.

Risk No	Relative loss	Relative probability	Relative exposure
1	1	1	1 (Low)
2	2	3	6 (High)
3	2	2	4 (Medium)
4	2	1	2 (Low)

Table 2: Sample of qualitative assessment of risks

The relative exposure of risk shows basically the risk importance. The higher the relative exposure is, the more exposed our project to that risk is. In our table for instance is clear that risk 2 is the most severe and risk 1 the least severe. Usually the relative exposure is presented with different colors based on the criticality of the risk in order to highlight the most critical one. The relative exposure that has values 1 or 2 is presented with green colour indicating low exposure, values 3 and 4 are highlighted with yellow indicating medium exposure and values 6 and 9 with red indicating high exposure. Also the relative exposure in some cases is described with text corresponding to the product values and can be "low", "medium" or "high". The highlight or phrasing of the relative exposure aims to provide guidance based on which after the completion of this phase we prioritize the risks and we decide which of them will be proceed to further quantitative examination as we see in the next section. The number of selected risks for further consideration also depends on the type of organization and project, nevertheless the most common approach is to take the top ten risks with the greater impact for further examination.

Although this method seems to be easy to use and apply there are many disadvantages that might lead to inaccurate and erroneous results. Firstly this method is based on assumptions and therefore cannot be accurate and it is dependent strongly on the experience of the evaluator. Secondly each evaluator has to apply this method individually because there is not possibility to have an average of all estimates. Another factor that brings barriers to accuracy is that the scale of available values to be chosen is limited. In addition this method fits only to stakeholders that have experience in project risk management as Ericsson claimed, because not so experienced people struggle to provide the related loss and probability using the scale from 1 to 3. Usually all the stakeholders know intuitively if the risk is serious to be evaluated quantitatively or not, and the application of this step becomes many times redundant.

In addition this method is missing an important consideration that arises during the project risk management iterations. The biggest risks of complex IT projects and particularly financial IT projects have to do with economics and the economic impact. The assessment of the economic impact of risks along with a method which combines qualitative with quantitative assessment which we call "perceptive" is discussed in the section "Perceptive Method".

3.4. Quantitative Assessment of Risks

"You can use all the quantitative data you can get, but you still have to distrust it and use your own intelligence and judgment."
Alvin Toffler

The quantitative assessment of risks is one of the most demanding phases of the risk management iteration and requires significant experience skills and sometimes statistical data. In this section we clarify the issues concerning the traditional estimation method of quantitative risk analysis. We describe in details the quantitative assessment starting with the analysis of the triple estimation method, continuing with the examination of the skewness effect of the loss distribution. In the last part we cite a new technique of risk assessment that we call "perceptive" which aims to introduce a new approach on how to assign likelihood to specific types of risks and combine qualitative and quantitative assessment by transforming words to mathematics.

3.4.1. Triple Estimation Method

In this subsection we describe the quantitative assessment of risks by using the triple estimation formula [9] and some issues and inaccuracies concerning to its application.

When the risk identification and prioritization phase are finished the risk facilitator with all the evaluators estimate the expected losses as a result of the potential adverse event. An evaluator can be any stakeholder that participates in the risk evaluation process. The base estimation method is the three-point estimation technique according to which evaluators are estimating the *min*, *most likely* and *max* expected losses. Usually the [min, max] interval is given with 99 percent confidence level, which means that the likelihood of real loss is out of that interval is estimated to be only one percent. The *min* of estimated minimums is taken as the lowest value of expected loss. For instance if we have four estimators and they provide such values for *min*, [0, 10, 10, 8], then we are taking the minimum of all estimates, which in this case is 0. The principle is the same with choosing *most likely* and *max* estimates. *Most likely* value is the average of all estimated most likely values and the *max* is the maximum of all estimated max values. Whenever we have all the estimates we can calculate the *min*, *max* and *most likely* values. The table below visualizes our example:

	Min (TSEK)	**Most likely** (TSEK)	**Max** (TSEK)
Estimator 1	0	50	120
Estimator 2	10	50	130
Estimator 3	10	65	160
Estimator 4	8	65	120
Estimate	0	57.5	160

Table 3: Sample of quantitative assessment of risks

Having these results, we can apply the triple estimation formula by evaluating the expected *min*, *most likely* and *max* losses to calculate the average expected losses (*mean* value). Generally the *mean value* is the mathematical expectation of the loss distribution. In triple estimation formula it is defined as the weighted average of three (*min*, *most likely*, *max*) estimated values:

$$M = \frac{min+k*most\ likely+max}{k+2} \quad (2)$$

Here k is the weight of most likely value. In different practical situations the value of k is different. For instance in estimating the lines of code of the software that must be implemented, weight is assigned $k = 4$ [16]. In estimating preliminary cost it is usually $k = 3$ or in some special cases $k = 2.9$ [9]. In Ericsson Money Services they use $k = 2.9$ value:

$$M = \frac{min+2.9*most\ likely+max}{4.9} \quad (3)$$

Thus using this value for our example we get:

$$M = \frac{0+2.9*57.5+160}{4.9} = 66.7$$

Besides the estimated average loss we also need to calculate the dispersion which is another indicator of risk exposure. The greater the dispersion of estimated values from *mean* is, the more uncertain the adverse event is and its consequences. The dispersion can be expressed by *standard deviation (D)*, the simplified calculation of which is:

$$D = \frac{max-min}{4.65} \text{ [9]} \quad (4)$$

If we calculate *standard deviation* by this formula for our example we get:

$$D = \frac{160-0}{4.65} = 34.4$$

Usually when we assess the severeness of a risk we take into account those two major indicators, the average loss (M) and dispersion (D). Nevertheless there are other important factors that we must not neglect such as the risk tolerance of the organization, the volatility of hazardous event (described in "Monitoring and Control" section), the type of loss distribution and so on.

Despite the simplicity of the triple estimation formula while assessing the risks we have some serious issues regarding the type of loss distribution. Usually the density function indicates the type of the curve that the loss as a random variable is distributed. In here the loss distribution is confined with the interval of *min* and *max* values, is discrete and expressed in terms of money. Generally in assessing risks and using the triple estimation formula we use the *Erlang distribution*. The probability function of which is given as:

$$P(loss) = \frac{\lambda(\lambda * loss)^{n-1}}{(n-1)!} e^{-\lambda * loss} \quad (5)$$

λ is the rate parameter and n is the shape parameter. [4]

The experience shows that in most of the hazardous situations the estimated losses fitted to an Erlang distribution can reflect the real losses when we use formula (3). Notwithstanding, there are some specific cases when the loss distribution is significantly different from Erlang distribution and has noticeable skewness.

In the next subsection we focus on the issue when the real loss distribution is significantly different from the Erlang type. We show that in such cases we must carefully examine the risky event and choose a different value for the weight of most likely value to avoid erroneous estimations and compensate the distribution skewness effect on formula (2).

3.4.2. Skewness Effect on Mean Value

"Creativity is the ability to introduce order into the randomness of nature"
Eric Hoffer

As we have described in the previous subsection in most cases we can adapt the Erlang distribution to resemble the real distribution of losses. But the term real distribution is also conditional because we do not have the same statistical population to assess what type of curve we have. However the experience of a number of scholars and practitioners shows that Erlang distribution can be successfully applied in the software development industry while assessing preliminary costs and risks [4]. Nonetheless there are some special cases when the use of Erlang distribution brings some significant divergences of evaluated mean value from real mean value of the distribution. The result can exacerbate dramatically when the distribution curve has absolute skewness, that is, either left or right tail of the distribution curve is missing (Figure 3). In such cases a risk manager must ponder for the use of the triple estimation formula:

$$M(x) = \frac{min + 3 * most\ likely + max}{5} \quad (6)$$

Figure 3: Probability - Loss distribution curve without left tail

As Professor Steen Lichtenberg describes [9], if the real distribution is quite close to Erlang then the magnitude of the error is not conspicuous and does not put a risk facilitator in a plight. Practice shows that those kinds of errors are much less than the errors emerged from bad estimates and insufficient decomposition of complex task for estimation. However it is not unimportant and we should be careful while assessing the actual risk. Much complicated and competitive task is when it is difficult to decide which kind of distribution we deal with. We know that mostly we can fit it to Erlang but dependent on uniqueness of the risk and uncertainty parameters, the distribution type can be quite far from Erlang type.

Whenever we have symmetric distribution we do not pay attention what the distribution type is because anyway the triple estimation formula is not affected at all. In such cases the mean value (M) coincides with most likely value. To describe with statistical terms, the *mode* and *median* of the curve are the same. For instance if we have 10, 40 and 70 values for $min, most\ likely$ and max values conformably, then the *mean* equals $M = \frac{10+3*40+70}{5} = 40$. The picture is the same if we change the weight of the *most likely* value and take some arbitrary value. For instance if in formula (2) we substitute $k = 3$ weight by $k = 3.6$ and so $k + 2 = 5.6$ instead of denominator 5 the result remains the same, 40 as we see in Figure 4.

This effect can be generalized as follows: Any type of distribution that is symmetric to $x = median$ line, the *median*, estimated *most likely* and *mean* values coincide, and triple estimation formula is applicable effectively.

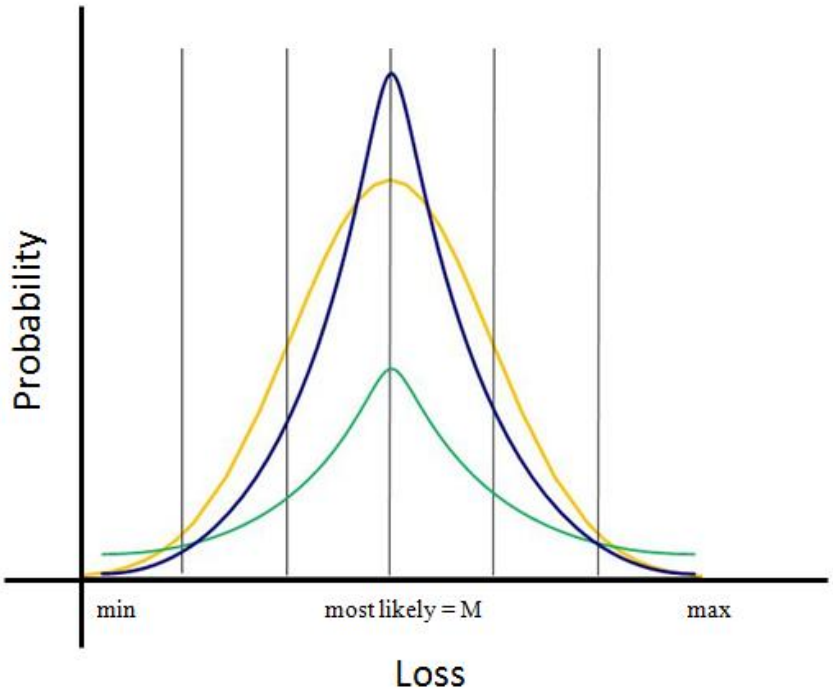

Figure 4: Symmetric Probability – Loss distribution curves

As the difference between $(most\ likely - min)$ and $(max - most\ likely)$ is getting greater, the distribution type is getting more important. The reason is that the weight of the most likely value is varying. As we have mentioned earlier when we have Erlang distribution the formula (2) is still applicable in most cases (some exceptions can happen due to change of *shape* and *rate* parameters of the Erlang distribution [4] especially when *most likely* value is equal to either *max* or *min* values), but when the distribution is *more convex* or *more incurved* then the weight of the *most likely* value must be changed in the formula (2).

In practical situations there are some cases, that likeliness of estimated *max* value and some closer values to it are still not as possible as the *most likely* value but have significant probability. For instance, if we park our car outside on the street, then there is likelihood that the car will be stolen in the night. The maximum estimated loss is our car price. But most likely the car will not be stolen. Now if we change our mind and park our car in the parking lot there is still likelihood that the car will be stolen. It is possible but much less probable than in the first case, as it is under the surveillance of the guard. Despite of the same *min*, *most likely* and *max* estimated loss the average estimated loss is different. The reason is the likeliness of the *most likely* and *max* estimated losses differs. In this example we have a kind of "either-or" type of event and the reader may think we do not have distribution curve at all, only two possible cases – either car is stolen or not. But if we imagine that there is a public disorder in the street and they can harm the car, then we have a loss distribution as they might cause some damage which can be expressed in terms of money. They can break down the car windows, damage the metal, burn it and so on. All

those damages can be expressed in terms of money. On the loss distribution we have $min = 0, most\ likely = 0$ and $\max = car\ price$ ($most\ likely$ loss can be some other value also). In this simplified example we can see that the *min, max* and *most likely* values are the same, but we feel safer to pay some money and park the car in the parking lot as inside parking lot the most likely estimate is more trustworthy to happen than outside of it. This fact can be expressed statistically by changing the distribution curve.

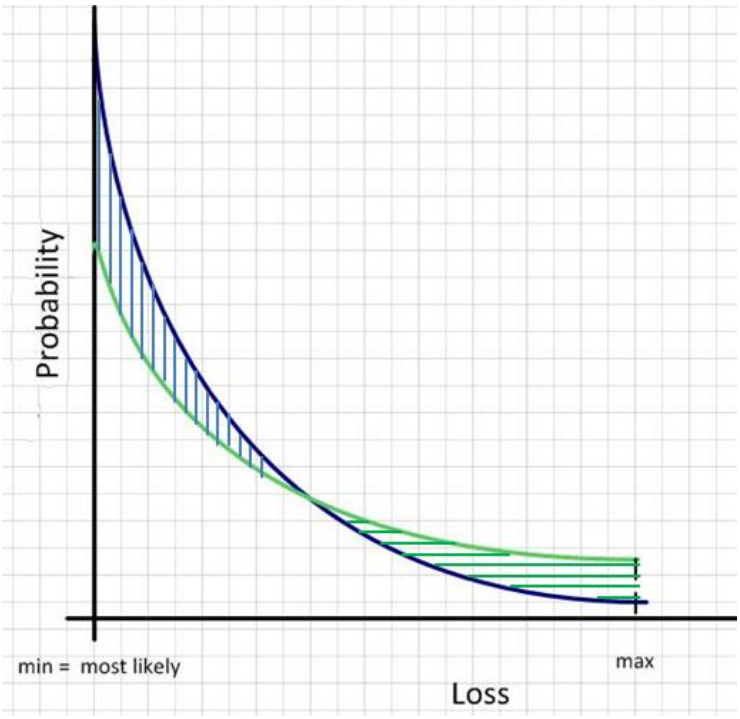

Figure 5: Car example: Probability – Loss distribution curve

In Figure 5 the blue curve expresses the state of the car in the parking lot and the green curve for outside correspondingly. This effect is also very interestingly expressed by the surface of the curves confined with the axis of loss. We know that cumulative distribution function can be presented also with the surface of the area confined by probability density function and axis of losses as a random variable and it must be equal to 1 from the condition that cumulative distribution function is the integral of the density function. Now if we compare the surfaces of the curves we notice that even with the same *min, max* and *most likely* values, when we park our car in the parking lot some part of the density function's surface is moving to left thus reducing the overall exposure. In Figure 3 the initial surface is green which after mitigation and distribution changes moving to blue side thus showing that the most likely and some closer values are getting more probable reducing the probability of the *max* value and some closer values of it.

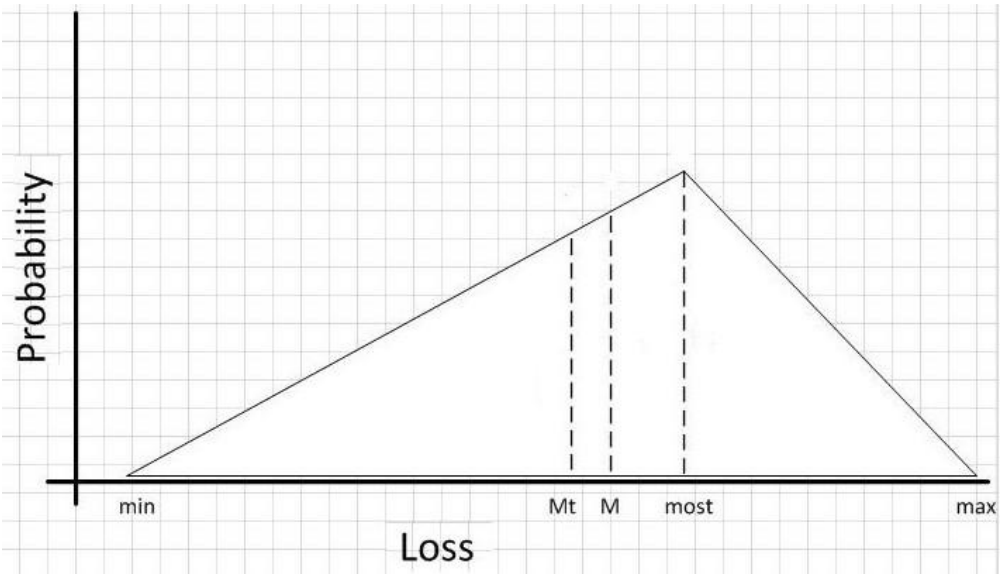

Figure 6: Triangular Probability – Loss distribution

Examining the risky situations that can arise in financial IT projects such as Ericsson Money Services we found that the upper observed issues are largely possible. Possible project fulfillment delay and the penalties because of it can be a good example. This and other type of risks sometimes cannot be described with Erlang distribution. In such cases when we have more convex (usually before mitigation) and more incurved (usually when we mitigate and evaluate the possible losses again) distributions, we must find other type of distribution to describe loss distribution.

As a special type of any other convex distribution the *triangular distribution* can be applied emanating from the simplicity of the distribution parameters [4][5]. Comparison of distribution parameters, particularly the mean value can give some valuable results. The mean value (M), which is the *median* for triangular distribution (*), is:

$$Median\ (M_t) = \begin{cases} min + \sqrt{\frac{(max-min)*(most\ likely-min)}{2}} & for\ most\ likely \geq \frac{min+max}{2} \\ max - \sqrt{\frac{(max-min)*(max-most\ likely)}{2}} & for\ most\ likely < \frac{min+max}{2} \end{cases} \quad (7)$$

*In statistics the *mean* value or *expectation* value is sometimes referred as the arithmetical mean of the set of values and sometimes the weighted mean. *Median* is the point where the total surface of the density function curve is equally shared. This express the fact, that the probability that the random variable will drop in the left side of the *median* equals the probability that the random variable will drop in the right side of *median*. When we refer *mean* value in the triple estimation formula we mean the *median* of the distribution.

For example if we have such estimations

$$min = 10, most\ likely = 80, \max = 100$$

Then the estimated mean value by triple estimation is:

$$M = \frac{10 + 3 * 80 + 100}{5} = 70$$

Now if we count the mean value by using the formula (7) we get:

$$M_t = 10 + \sqrt{\frac{(100 - 10) * (80 - 10)}{2}} = 66.1$$

As we see the two results differ. The real mean value is less than the value counted by triple estimation formula. The divergence reaches to its worst case when we have most likely value equal either to *min* or *max* values. For instance:

$$min = 20, most\ likely = 20, max = 150$$

$$M = \frac{20 + 3 * 20 + 150}{5} = 46$$

$$M_t = 150 - \sqrt{\frac{(150 - 20)(150 - 20)}{2}} = 58$$

As we see the difference between M and M_t now is significant. The further the most likely value is from the median of the distribution the greater the divergence between $M_t\ and\ M$ is. When the *most likely* value is closer to *min* value (right skew) then $M_t > M$, when *most likely* value is closer to *max* (left skew) value then $M_t < M$**.** The worst case is when *most likely* equals either to *min* or *max*. In case of the symmetric distribution the triangle becomes isosceles and those values become equal.

In such cases when we have more convex distribution than the Erlang distribution is, particularly triangular, we need to reduce the weight of the *most likely* value in the formula (2). For instance if in previous example we substitute the weight of the *most likely* value $k = 3$ with $k = 1.5$ then we get:

$$M = \frac{20 + 1.5 * 20 + 150}{3.5} = 57$$

This approximation is quite close to $M_t = 58$ value, which can be regarded as a good estimate.

Unfortunately neither the distribution type nor the skewness effect can be defined precisely for a specific risk and nowadays there is not any generalized approach to apply but it does not imply that their effect on estimation must be disregarded. On the contrary, these effects sometimes are very visible depending on a specific situation and can be reduced significantly.

In the example of the parking we noticed that whenever the car is in the parking lot the *max* estimated loss is still the price of the car, but it is not worryingly probable. In such cases when the *most likely* value and some closer interval to it is much more likely than the values situated close to the edges of the interval, can be called more incurved than the Erlang distribution. The Gumbel [11] or skew-Laplace [1] distributions can serve to describe the probabilistic behavior of losses in these situations. Sometimes in a specific situations when *min* and *most likely* estimates are the same the exponential distribution can also serve us as it is a simplified version of Laplace distribution [4] (when we remove the location parameter from the later one).

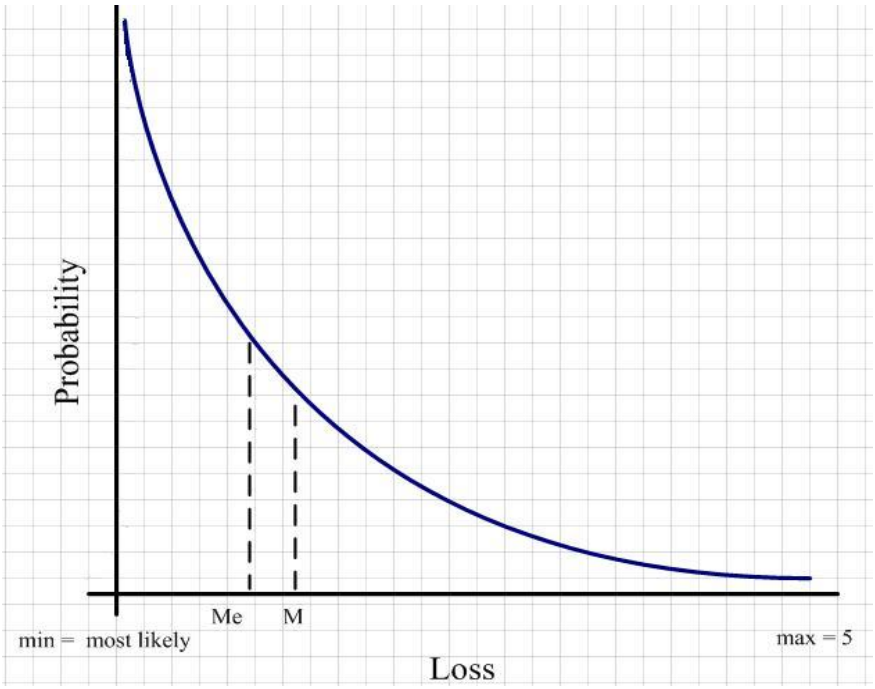

Figure 7: Exponential Probability – Loss distribution

In practice to adapt losses to one of those distributions is a difficult task because of the exponential form of the skew-Laplace, double exponential form of the Gumbel and adjusting *min, most likely* and *max* values with scale and location parameters and specifying confidence level interval. These issues are not addressed in our work. But we discuss one example of exponential distribution to show that the skewness effect has contrary effect compared with triangular distribution. In the parking example when the car is in the parking lot and safe, the re-estimated losses can be presented with exponential curve as the *most likely* and *min* values are

much more probable than *max* or some closer values. The probability density function of exponential curve when we have x random (in our case losses) variable is:

$$f(x,\lambda) = \begin{cases} \lambda e^{-\lambda x}, X \geq 0 \\ 0, X < 0 \end{cases} \quad (8)$$

$\lambda > 0$ is the rate parameter of the distribution [4].

Specifying a value for λ, for instance, λ=1, we get such results:

$$x = 0, f(x,\lambda) = 1$$

$$x = 1, f(x,\lambda) = 0.37$$

$$x = 2, f(x,\lambda) = 0.136$$

$$x = 3, f(x,\lambda) = 0.05$$

$$x = 4, f(x,\lambda) = 0.0185$$

$$x = 5, f(x,\lambda) = 0.007$$

Observing the results we can easily conform that those can quite closely approximate the real loss distribution because the probability of no damage (*min*, *most likely* values) is very high and it dramatically diminishes when the estimated losses are approaching to car price. At the point of 5 TSEK which is the car price we have 0.007 probability of loss: An estimate that ensures a bit more than 99% confidence level (apparently in this example we cannot lose more than our car but in a program, while estimating potential risk exposure, the likeliness of greater losses are possible, which are out of 99% confidence level and thus disregarded). Now if we compare the mean value, calculated by the triple estimation formula (M), and median of the exponential curve (Me), we can see the differences.

$$M = \frac{0 + 3 * 0 + 5}{5} = 1\ TSEK$$

The median of the exponential distribution is:

$$Me = \lambda^{-1} ln2 = ln2 = 0.693\ TSEK$$

This difference is visualized in Figure 7. The real risk exposure value is 0.693 TSEK whereas with triple estimation formula we have 1 TSEK.

And again if we chose a different weight for most likely value, say $k = 5.2$, we will have:

$$M = \frac{0 + 0 * 5.2 + 5}{7.2} = 0.694\ TSEK$$

With *k=5.2* weight of *most likely* value M_e and *M* values are almost equal.

In different situations and for different type of risks the distribution curve can change its shape widely. Our research shows that those changes are most crucial on triple estimation technique when we have sharply emphasized skewness of the distribution. The skewness effect reaches its highest magnitude when the *most likely* estimated loss is equal to either *min* or *max* values. Depending on which side of the distribution is the skew and what type of distribution is the relationship of real *mean* value (*median*) and *mean* value of triple estimation interrelate the following way:

- Left skew and more incurved than Erlang – $M<M_{real}$
- Left skew and more convex than Erlang – $M>M_{real}$
- Right skew and more incurved than Erlang – $M>M_{real}$
- Right skew and more convex than Erlang – $M< M_{real}$

The examined examples and calculations of mean value according to different known distribution curves showed us that the weight of the *most likely* value can change in 1.5 to 5 interval (even in greater interval in some critical cases are possible).

We also noticed that choosing the distribution curve to resemble the real hazardous situation is not an easy task but it is undoubtedly possible if we examine that situation profoundly (comparing likeliness of different estimated losses by our inner perception and specifying the distribution curve or the weight of *most likely* value).

We must always remember that mathematical equations and geometrical forms (such as distribution curves) are a unique type of language created for resembling the natural phenomena. In reality the essence and the behavior of the event is always different [14]. The trick is to understand when and how we can apply already discovered shapes and formulas to overcome our specific problem. The more we are aware of statistical data, current condition of reality and how they are interrelated the more precise we will be in our predictions. In order to success on this we would better to set us free from our desires, delusions, pessimism, conditionalized manners, business values and other hampering feelings and possessions, set our mind free from biased, preconceived and disposed attitude to the event and evaluate consciously and freely.

3.4.3. Perceptive Method

"When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind;"

Lord K Elvin

Widely speaking about risk management in practice we often encounter a situation when the expectance of adverse event has two possible outcomes – either occurrence or not occurrence. To clarify this statement we can compare the example *Risk 2* discussed in section 3.2 and the example of possible stealing the car discussed in subsection 3.4.2. For instance when we know that the possible exchange rate variation between YEN and GBP may threaten the expected profit of Ericsson Money Services we must estimate not only if the exchange rate variation may occur but also how much the magnitude is of the variation. The loss of profit is highly dependent of the magnitude of variation. Conversely in the second example when we park our car outside then we have the odds to lose our car or not as it either can be stolen or not in the night. There are two possible outcomes of this risk and the magnitude of the loss is the same as the car price. The similar risky situation is, for instance, paying penalties because of delayed delivery of a software product. When there is a fixed date for delivering a product the possible delay costs certain amount of money and depending if the product is delayed or not the organization ought to either pay or to not to pay the penalties. These kind of risks are usually called "either-or" because of theirs two possible outcomes. As we discussed in subsection 3.4.1 the estimation of these risks by triple estimation method can bring erroneous results because of skewness effect of loss distribution. When we have two possible expected outcomes of adverse event the estimated most likely value of the risk is equal to either min or max values. We cannot disdain the effect of skewness especially when we have two possible values of occurrence as we have shown in subsection 3.4.2. In such cases the triple estimation formula can only be used when we know with a sufficient approximation of what type the loss distribution is.

The traditional way of risk assessment is to estimate the probability of the occurrence of adverse event, the impact of it in terms of cost and multiply these two values in order to get the exposure of a particular risk:

$$E = P * I \qquad (9)$$

P – Probability

I – Impact or Loss in terms of cost

E – Risk Exposure which shows average loss in terms of cost

Despite the endeavor of the estimators some practitioners mention that it is very hard to estimate the probability of an event occurrence when we do not have the same statistical population. The main problem is that the estimators cannot see clearly the likeliness of the event behind a

number. For instance when we ask an expert how much the probability that the actual costs of the system maintenance will exceed the foreseen cost by 25% is he may face difficulties to put his perception of likeliness of that event into a number such as 0.3 in a scale from 0 to 1. Usually in real life situations while assessing any uncertainty we estimate the probability with natural language such as "possibly", "may be", "certainly" and so on. But on the other hand in order to be able to estimate quantitatively we need a number for probability to multiply with expected losses. Whenever we are asked to estimated the probability of the occurrence of an event it is assumed that we have some statistical population behind it from which we can derive a number. But as we know and the experience of Ericsson shows in some cases it is very time consuming to collect the possible statistical data and frame it, or even in most cases we do not have relevant statistical data at all. Particularly in software projects' risk management when it comes to quantitative assessment of risks some practitioners assess the emerged risks qualitatively or in some cases they apply the triple estimation formula as it is proven to be consistent and trustworthy [2].

The idea of creating the perceptive method is to have a standard technique which can simply and effectively deal with "either - or" types of risks by applying probabilistic estimation in order to avoid both the skewness effect of the loss distribution, while assessing by triple estimation formula, and the difficulties of the estimators, while they are required to give a certain probability of the adverse event's occurrence. This method is based on human experience and inner perception of the reality which does not necessarily rely on how many similar events we have experienced heretofore but the ability to analyze and deduce results from any possible data that is available in human mind and has a connection somehow with the expected event. For instance if we are asked to evaluate how much the likelihood is that tomorrow will rain we do not count all the days during the year that was rainy and divide on the number of days of the year. We usually look up to the sky trying to understand the humidity of the air, if there are clouds or not, if it is windy or not, compare with newspaper prediction and we eventually say – "doubtfully". All our knowledge, experience and ability of deduction come and concentrate in this single word which expresses our inner perception of the reality by analyzing not only the statistical data about the fact (we are in England and so it must be rainy by probability of 0.7), but also all the current condition of the reality and its tendency to the next stage of the time. If we were, for instance, people of ten thousand years ago we definitely would have difficulties by judging based on windiness or humidity and no newspaper would be available, but now, when all the information has transferred to us how to make decision based on all this data we are able to assess the reality much better. Thus the competence of the method relies on the human experience that has been accumulated during ages and does not imply having the same statistical population to estimate the likeliness of the event.

As we know the natural language is one of the most powerful tools to share our knowledge and have common sense with other people on how the reality behaves. When we are asked the question "do you think it will rain tomorrow?" and we answered "doubtfully" it is common

knowledge between asker and interlocutor and it is perceived as "I have no obvious reason to be believe it or not but I have slight knowledge by judging the situation and I believe that the tendency of the reality is slightly prone to not having rain tomorrow". This is kind of explanation of the word "doubtfully" that we have perceived and articulated.

Based on this judgment and analyzing more than 200 adverbs, adjectives and combinations in English, examining the most popular dictionaries of English and discussing with philologists we have chosen the most suitable and appropriate words to express the likelihood of expected event that is understandable enough for the estimators and practitioners. Meanwhile we have chosen the likelihood expressing adverbs and adjectives in a way that it allows us to assign the corresponding probabilities to these words in terms of numbers in a good enough approximation. The reasons of this idea are to assess the likelihood of the event in natural language, that is easier and understandable for people and to have quantitative results in the end, to be able to assess the expected exposure of risk quantitatively.

Below we focus on the delineation of the chosen words and theirs probabilities one by one reasoning the rationale of adopting it:

The upper and lower boundaries of the likelihood are the 98 % and 2% of the chance of event's occurrence. These numbers show that the evaluator has several facts that strongly imply the occurrence or not occurrence of an event and there is no visible reason to think otherwise. But as the event is probabilistic and the condition of reality can be changed for unknown reasons the evaluator does not give 100% or 0% chance of occurrence. For this likelihood we denote the following combinations:

"$Almost\ certain$" $= 0.98$

"$Almost\ impossible$" $= 0.02$.

When we say that an event is almost certain that will happen we do not have doubt but we know that the event is probabilistic and there is a slight possibility that an unexpected hap can change the conditions.

One step lower than "Almost certain" and one step above than "Almost impossible" we use:

$Highely\ likely = 0.86$

$Highely\ unlikely = 0.14$

When we say that the event is highly likely to happen then we believe that there is strong evidence from all the possible facts and observations that it will happen but at the same time there are some very little but visible factors that might prevent the occurrence of it. Sometimes depending on the situation, our profession, our attitude to the reality or the way of perceiving the reality we use some other alternative words instead of "highly likely" such as "evidently",

“obviously”, “apparently”, “manifestly” and so on. All these mentioned words are anyhow dependent on how we have perceived the necessary information to make a decision. For instance the word “evidently” is mainly based on the not subjective, common observation and alternatively the word “apparently” is based on the visual subjective observation. In both cases the occurrence of event can be considered as quite probable but the word combination “highly likely” does not imply how is the information observed or perceived it just state the fact the something is highly likely to happen and other all the detail deductions are hidden in the evaluators head. The same way we can use “hardly ever” or “rarely” instead of “highly unlikely”. Especially the adverb “hardly ever” can substitute successfully the combination “highly unlikely” but for the cohesion of the list we choose the later one.

Less probable than “highly likely” and more probable than “highly unlikely” we denote the following adverbs:

$"Probably" = 0.74$

$"Improbably" = 0.26$

These two words we use frequently in daily speech. Whenever we express our attitude to the event that something “probably” will happen (not something is probable to happen) we give about 75% chance that it will happen. In dictionaries mostly the meaning of this word is described as to be quite positive to the event that it will happen but not sure of it. The adverb “improbably” quite closely approximate the converse likeliness of the “probably” which means that when we say an event improbably will happen we mean that there is approximately 25% chance to happen.

As less probable adverb than “probably” and more probable word than “improbably” we have conformably:

$"Possibly" = 0.62$

$"Doubtfully" = 0.38$

The word “possibly” has a special power to indicate that we do not have any obvious reason for believing that an event will happen but there are some hidden or not evidential reasons and that makes us to preconceive that the event is disposed to happen. The same way when we say “doubtfully”, we do not have any visible evidential superposition of facts to deduce a stronger attitude of acceptance or rejection of event occurrence, but we still believe that we perceive some indirect information from the reality that says the event is more possible not to happen rather than happen. In this condition we clearly believe that odds are not equal. In some cases we use “maybe” instead of “possibly” which shows slightly lower chance for event occurrence than the adverb “possibly”.

And eventually we have the position that we do not have any information about the system and we are completely unaware what can happen. The likelihood of this can be assigned as:

$Fifty/Fifty = 0.5$

Usually the more the facts, evidence, observations are and the less the misleading knowledge is about the reality, the stronger our belief is about event's occurrence. In *Information Theory* when we do not have any information about a system it means the entropy of the system is the highest and the probability of occurrence of an event in the system is regarded 0.5. Therefore there can be two possibilities, either we need to observe further and have considerably more information to assess the likelihood better or we believe that it is not possible to have any evidence about the system or the situation and we estimate the probability as fifty/fifty. This is a common term that we always use in our daily life which means that we do not have any obvious information to be slightly disposed to positive or negative answer to the happening of the event. After these denotations we have the full list of the probabilities and their assigned values as we present in the table below:

Likelihood by Natural language	Likelihood by numbers
Almost certain	0.98
Highly likely	0.86
Probably	0.74
Possibly	0.62
Fifty/fifty	0.50
Doubtfully	0.38
Improbably	0.26
Highly unlikely	0.14
Almost impossible	0.02

Table 4: Perceptive key words and assigned probabilities

All these nine words and their assigned probability values allow us to express our perception of likeliness of an event's occurrence and transfer that perception to a number in order to evaluate the likelihood quantitatively. In other words we express our attitude by human language and convert it to the language that the nature speaks. We have chosen the words in a way that does not have multiple meanings or too wide range for expressing likeliness which can cause erroneous results. A supportive condition is that the user must express his/her perception of likeliness having all these words in front of him/her so it will be easy to understand more precisely the meanings. However we strongly believe that during the evaluation the users should not see the numbers with these words and it must be hidden until the evaluation process is finished and we need to count the average of the results. We advise that the estimators should not think too much about the word and about how much the assigned number is. They must choose spontaneously the word that is the closest characterizing likelihood of the event.

Below we cite a clarifying example of the method:

Suppose we have four evaluators and they must predict the likelihood of the event whether tomorrow will rain or not. Every evaluator expresses his/her belief using the perceptive method (Table 5).

Evaluator name	Likelihood
Evaluator 1	Doubtfully
Evaluator 2	Doubtfully
Evaluator 3	50-50
Evaluator 4	Improbably

Table 5: Evaluators estimations based on perceptive method on the raining example

After the evaluation we can assign the corresponding values and calculate the mean value by calculating the sum of four assessments and dividing by the number of evaluators (Table 6):

Evaluator name	Likelihood	Likelihood
Evaluator 1	Doubtfully	0.38
Evaluator 2	Doubtfully	0.38
Evaluator 3	50-50	0.5
Evaluator 4	Improbably	0.26
Average		0.38

Table 6: Assigned likelihood value based on the estimations of the raining example

The average likelihood is 0.38.

For assessing the risk exposure we need to calculate the average likelihood, the average loss and then multiply these two values. Suppose we are a software project development team and if we delay to deliver the product from the promised day we have to pay penalties. Table 7 presents the results of the evaluation.

Evaluator name	Likelihood	Likelihood	Impact SEK	Exposure SEK
Evaluator 1	Improbably	0.26	500000	
Evaluator 2	Highly unlikely	0.14	500000	
Evaluator 3	Almost Impossible	0.02	500000	
Evaluator 4	Almost Impossible	0.02	500000	
Average		0.11	500000	55000

Table 7: Product delivery risk example using perceptive method

As we see the cost of penalty has fixed value and the only variable is the likelihood. This is also one of the special features of this method as it allows decomposing the likelihood and impact and

estimating separately as a contrast to the triple estimation method. When we have fixed value of loss in case of adverse event occurrence this method becomes more consistent.

In a common situation when the impact of risk is not fixed value it is useful to calculate *the most probable interval* of losses. To explain this concept, suppose we have the following situation: The Solution Design Program of Ericsson aims to develop a new mobile service in a fixed timeframe of one year. At the same time there is an expected reorganization in Ericsson which can have severe impact on the program if they do not finish the development and release of white label before the reorganization processes are begun. Suppose six evaluators are designated to estimate the exposure of risk in case of the product development is not finished before the reorganization. The table below visualizes the results:

Evaluator name	**Likelihood**	**Likelihood**	**Impact SEK**	**Exposure SEK**
Evaluator 1	Possibly	0.62	500000	
Evaluator 2	Probably	0.74	700000	
Evaluator 3	Probably	0.74	450000	
Evaluator 4	Highly likely	0.86	500000	
Evaluator 5	Probably	0.74	600000	
Evaluator 6	Possibly	0.62	800000	
Average		**0.72**	**591666**	**426000**
Min		**0.62**	**450000**	**279000**
Max		**0.86**	**800000**	**688000**

Table 8: Solution Design Program example using perceptive method

The minimal exposure is calculated as the minimal estimated likelihood multiplied by minimal estimated impact among all estimates. The same way we calculate the maximum exposure. The interval of [min exposure, max exposure] we call the most probable interval of losses. For our example it is [279000, 688000]. The greater the interval is the more unpredictable the risk is irrespective of the average exposure.

In this method the usage of words is tightly chained with how cognizant the user is about its meaning in the evaluation context. In different geographical areas different people can use the same word with some divergence of the meaning and this can become a hindrance of its application. Nonetheless the words are chosen in a way that it reduces this effect maximally and we provide self-explanatory texts with every word as an augment or supportive function. To use the method it is worth to have a compendium of our self-explanatory texts with every keyword in the list that we propose in this framework. In case the user does not feel comfortable with a certain word he/she can read about the word explanation in terms of expressing likelihood. The application of the method is experimentalized with both experts and non experts in different fields for estimation the probability of variety of events and consolidated to be easy graspable. Before applying in real-life problems as a new method it must be epistemologically consistent to distinguish the justified belief from subjectiveness. To be so we propose to apply it parallel with

the other well known risk management methods and adverse events' outcomes and collate results later in order to judge about the competence of the method.

The disparity between real likelihood and assessed likelihood is estimated not to be considerably big in project risk management as the natural language supports at least nine or ten words in probability [0, 1] interval. The worst case of the divergence between real likelihood and assessed one is estimated to be 6% of overall estimated cost while calculating risk exposure value. When we feel that we want to assign a different probability than the proposed nine key-words, for instance, something between "probably" and "highly likely" we are not able to do it directly and perhaps in most cases we do not need to do, because the numerical difference between this two words are 0.12. The worst case of divergence arises when we strongly believe that we assess the probability of event as between "highly likely" and "probably" which is just the midpoint of 0.74 and 0.86 and equals to 0.8. In this case we have 0.06 unit divergence and that comes to 6% of the estimated loss. If we have safety critical systems we never accept this value but we also know that in such systems other methods are used [3] [8]. In projects risk management when we usually evaluate the expected losses in terms of money by triple estimation method, traditionally or even qualitatively we usually accept greater interval of divergences. In case of triple estimation method this divergence emerges because of the loss distribution skewness effect or when we apply traditional method we estimate the probability by giving just a number that is mostly hardly graspable for the evaluators. Sometimes we even do not give a numerical value in case of qualitative assessment. The perceptive method somewhat combines the quantitative and qualitative assessment of risk as we express our perception of reality by natural language and later transfer it to the language of mathematics.

The congruence between words and likelihood and the appropriateness of theirs usage is adjusted by discussing it with the philologists, other experts and using the most trustworthy dictionaries (Collins and Oxford).

In the coming section we focus on the different types of strategies that can be planned when the risk is identified, assessed and we need to deal with it.

3.5. Risk Response Planning

"It is sometimes an appropriate response to reality to go insane"
Philip. K. Dick

Once a risk has been identified and evaluated, a response plan has to be specified in order to reduce or prevent the expected loss of that particular risk. In risk management the risk response planning is expressed as a mitigation activity. *Mitigation activity is the action that we perform in order to relieve our properties and goals from a risk partly or completely.* The mitigation activity can follow a certain strategy which is called mitigation strategy. A *mitigation strategy* is a conceptually specific approach to deal with emerged risks. In this section we cite the different

types of mitigation strategies and we discuss the different cases of response that each mitigation strategy applies.

Risk management is very flexible in terms of risk response planning due to the variety of available options in terms of mitigation activities. As every risk has its uniqueness and particular characteristics it can be faced in different ways such as acceptance, reduction or transfer. The mitigation activities are dependent on the characteristics and source of the risk, different resources and tools, the urgency of dealing with the risk and to who is responsible to deal with it. A mitigation activity can consist of different mitigation strategies which are the mitigation alternatives as we discuss in the coming section of risk analysis. Ericsson as well as most of the software organizations uses five different mitigation strategies which are the most common ones in the field of risk management [12]. Taking into account the fact that financial IT projects have more unstable parameters of risks and involve different business partners during the project development and the whole project life cycle, our approach to risk response planning contains seven different mitigation strategies. These seven mitigation strategies we describe below in combination with a simple life time scenario.

- **Risk acceptance:** In this case we accept the existence of the risk and we either ignore or accept the possible loss. For instance, we want to have picnic outside tomorrow but this night it is snowing and the weather forecast is not encouraging at all for tomorrow. Despite the discouraging weather condition we contemplate and decide to go for the picnic.

- **Risk avoidance:** It determines that we perform the necessary activities to avoid the risk occurrence. We modify the initial plans to cancel risky decisions or remove risky elements. For instance we know that there are sharks in a specific beach and therefore in order to keep ourselves in the safe side we do not go to swim there.

- **Risk reduction:** It describes the performance of specific activities to reduce the probability and impact of the risk to occur. For instance we have a tough exam next week and if we do not study hard there is a high probability to fail and moreover, to extend our studies till the retake date in August and therefore we may postpone our graduation and spend more money for rent. Therefore to reduce the risk's probability we decide to study hard for the whole week till the exam.

- **Risk mitigation:** We perform the necessary activities to eliminate completely the likeliness and loss of a risk. For instance suppose there is a probability that if we do not water the plants in our balcony while we are on vacation they will fade out and we have to spend money to plant new ones. Therefore we ask the neighbour to come ones and take care of them until we are back from vacation.

- **Risk transfer:** In this case we transfer the risk to another person or organization by signing a contract or buy insurance. In most of the IT projects the risk transfer is achieved by buying

an insurance to determine that someone else will deal successfully with our risk. For instance, thieves got inside our house during the vacation period and they stole belongings that cost 40.000 SEK. Nevertheless, because we wanted to avoid risks of such situations we have bought insurance for our house and belongings. Hence the insurance company has to pay us back 40.000 SEK. The risk transfer response is very common in financial IT projects where different operators are responsible for the normal operation of the system.

- **Risk coordinate:** In this case both the two parties co-operate in order to deal with a risk. It is possible in financial IT projects that both the developing house and the financial institute work together mainly by establishing an organization in between in order to carry on the necessary activities and deal with risks. A common risk of the developing house and the financial institute is agreed to be mitigated by the co-operation of the two.

- **Risk overlook:** In this case we identify inceptive events of risk but we do not plan any mitigation strategy and we simply examine the risk inceptive event against factors that can influence it. When we see that the hazardous situation becomes critical and needs mitigation then we plan which mitigation strategy to apply to deal with this particular risk.

Having all the possible responses to risks outlined above we recall the identified risks that we have defined at the identification section (Risk1 and Risk2) and we use them as example in order to plan a response. Both the two risks belong to Ericsson Money Services and by extension to Ericsson. Therefore Ericsson has to plan the proper response for each of risks. The two coming paragraphs describe the risk response plan for each of the two risks individually.

Risk one (Risk1) describes a situation where there might be a possible failure during the transactions between the central HUB of Ericsson Money Services and the two local ones in UK and Japan. A possible occurrence of this risk harms the reliability of the service and the normal operation of it. For the sake of reliability and normal operation of the service Ericsson plans to deal fully with this risk and applies the risk mitigation strategy. According to the risk mitigation strategy, Ericsson takes all the needed actions in order to eliminate completely the probability and loss of this risk and ensure the normal transaction of money between the HUBs.

The second risk (Risk2) describes a situation during which the exchange rate variation of YEN against GBP can cause loss of money of Ericsson. As we have discussed previously Ericsson Money Services is the first financial IT project of Ericsson and therefore Ericsson has no experience and is not able to deal with financial risks. In order to deal successfully with this risk Ericsson transfers the risk to a co-operative financial institute. This response strategy by Ericsson is defined as *risk transfer*. Ericsson negotiates with the partnering financial institution and establishes a contract to transfer the risk to the financial institute. Thus the financial institute is responsible to take all the needed actions in order to secure the profit of Ericsson through a transaction despite the changes of the currency exchange rate. Knowing that the currency

exchange rate between YEN and GBP can cause loss of money for Ericsson, they decide to interchange the profit of Ericsson in EURO. This response by the financial institute is called risk avoidance, because the financial institute decided to remove the risky elements which in this case are the exchange rate variation between YEN and GBP. The example was a simple presentation of how two organizations can negotiate and deal with a risk. In reality this process can be much more complicated and multi-action.

A risk response plan can be handled by combination of more than one different mitigation strategies as we have seen at the case of Risk2. Ericsson transfers the risk to the financial institute and after the risk is avoided by the financial institute. It is worth to mention that whichever mitigation strategy we apply to a particular risk, that risk has to be reported during the risk management iteration in order to be monitored and controlled and also track the risk's volatility as we see in the coming section. In the case that Ericsson has transferred the risk to the financial institute, the risk has to be reported within Ericsson and the financial institute has to inform Ericsson about the mitigation strategy that it applies to the risk and the performance of it.

Important factors that influence the activity of risk response planning and therefore the choice of mitigation strategy are the budget and the time planning of each project. Mitigation strategies can be judged as sufficient or insufficient depending on their cost and duration. Therefore a mitigation strategy that requires a significant budget and the duration of which exceeds the specified time frame is reasonable to be rejected. Apart from the correct selection of mitigation strategy it is important to be able to control and monitor the mitigation strategy in order to secure the successful performance of it. In the next section we describe the analysis phase and how to select the appropriate countermeasure in order to deal with risks.

3.6. Analysis and Countermeasure Selection

"An absolute can only be given in an intuition, while all the rest has to do with analysis."
Henri Bergson

One of the pivotal tasks in project risk management is to select and apply the optimum countermeasure against the adverse event. To do it so we organize and perform a mitigation activity. *Mitigation activity* is an activity that we perform in order to relieve our properties and goals from a risk partly or completely. In order to mitigate the risk the organization, project manager or risk manager may have several strategies. Each of these strategies requires different costs, and the risk exposure reduction is different according to selected strategies. *Any of these strategies with its mitigation cost and risk exposure reduction is a mitigation alternative.* We use the term mitigation strategy or mitigation alternative in the coming sections interchangeably. *Cost-effectiveness (CE) is a value in accordance with established criteria, which indicates how effective is the strategy to be applied for risk mitigation in terms of return of investment.* In

organizational project risk management the most effective way of choosing the best mitigation alternative is to analyze the cost-effectiveness of the chosen strategy. The best alternative is chosen as the alternative among all the selected or available alternatives which has the best cost-effectiveness value. In this section we discuss the importance of the unequivocal risk value and cost-effectiveness and we show how to establish it effectively avoiding errors.

Usually when measuring quantitatively how severe a risk is or as we are used to say how risky the situation is, we calculate the expected average loss. As we discussed in subsection "Triple Estimation Method", when we use triple estimation formula the average estimated loss (M) is considered a measure of risk. But it is not the only characterizing value of risk. We must take into account the dispersion (D) of the estimated values also. In this framework we define the *risk value* as a variable dependent on M and D parameters, loss distribution type and skewness of the distribution. This value is intended to represent the risk unequivocally and quantitatively. The risk value can be dependent on the risk tolerance of the organization, organizations attitude to the adverse event type, stability importance and so forth, but in our estimation method those factors are not taken into account. Alternatively we propose the risk facilitators to have their own judgment of those factors and make decisions.

Whenever we have calculated the mean value and the deviation of estimated losses we can have general idea how risky the situation is expressed in terms of money. The mean value shows how much we will lose in average. Statistically we can explain it as for instance if we have 100 similar risky situations we will lose in average approximately M amount of money. The outcome of this hazardous event may differ from expected M value dramatically. The main indicator of it is the *mean deviation*. The greater the deviation is the more the chance of having more diverged outcome from mean value is. Deviation is not the only indicator of unexpectedness of outcome of loss but it is the main indicator. Suppose we have estimated two risks by using the triple estimation method and calculated M and D parameters by formula (3) and (4) (Table 9):

	min (SEK)	**most likely** (SEK)	**max** (SEK)	**M** (SEK)	**D**
Risk1	0	20000	50000	22040	10752
Risk2	10000	20000	40000	22040	6451

Table 9: Sample of risk analysis

We have the same mean value of two risks which is 22040 SEK but the deviation of estimated losses for first risk is almost two times greater than for the second. This means that we know less information about the first risk (hazardous event) and the estimators have secured their estimates by giving greater possible interval of losses. The exposure of the first risk is greater because it is more unpredictable and the expected losses fluctuate in a greater interval. Whenever we have the same mean value with different mean deviations it is easy to differentiate that the one which has greater deviation value is more risky. But when the mean values are different it is difficult to differentiate the severeness of them.

To define the risk value unequivocally we need to consider about two factors:

- The risk value can be expressed by mean value plus some uncertainty caused by mean deviation that the real outcome of risk is different from mean value.
- The mean deviation expresses the uncertainty but the weight of it is different from mean value to be simply summed.

Comparing some estimates and results we propose to pick the $1/5$ as a weight index for the deviation. After this denotation we can write the formula for risk value as presented below:

$$R = M + \frac{1}{5} * D \qquad (10)$$

We do not take into account the risk tolerance of the organization, the volatility of it and other factors as it may vary from organization to organization and from situation to situation. Now the reader may wonder why we need to compare the risks and so to use this formula. In fact we do not need to compare two different risks but we do need to compare the same re-estimated risks in case of applying two or more mitigation alternatives. Suppose we have a risk that is estimated before the mitigation and re-estimated two times after specifying two possible mitigation alternatives.

Risk No 1	**min** (SEK)	**most likely** (SEK)	**max** (SEK)	**M** (SEK)	**D**	**R**
Without mitigation	20000	40000	100000	48163	17204	51603
Alternative 1	0	10000	10000	7959	2150	8389
Alternative 2	0	15000	30000	15000	6451	16290

Table 10: Sample of risk analysis using different mitigation alternatives

Judging from the results after applying these two available mitigation strategies and re-estimating the expected losses we see that the risk value in case of alternative 1 is two time as less severe as in case of alternative 2. If we do not spend money for applying those alternatives we must choose the alternative 1 to apply but usually when we foresee to realize a mitigation activity it costs some money: For instance buying insurance, paying for improvements of services, hiring necessary equipments and so on. To choose the best alternative taking into account the mitigation cost also we need to establish a cost-effectiveness indicator. Emanating from upper discussed results a good cost-effectiveness index can be the sum of mitigation cost and risk value:

$$CE = R + mitigation\ Cost \qquad (11)$$

We can judge based on this indicator how effective to apply a specific mitigation strategy is in terms of money. The mitigation alternative that has the lowest CE index is the optimal one to apply. If we complete Table 10 by providing the mitigation cost and cost-effectiveness index we get the following results:

Risk No 1	min(SEK)	most likely(SEK)	max(SEK)	M(SEK)	D(SEK)	R(SEK)	Mitigation cost(SEK)	CE(SEK)
Without mitigation	20000	40000	100000	48163	17204	51603	-	51603
Alternative 1	0	10000	10000	7959	2150	8389	10000	18389
Alternative 2	0	15000	30000	15000	6451	16290	2000	18290

Table 11 - Sample of risk analysis using different mitigation alternatives and cost-effectiveness

The mitigation cost of the first strategy is 10000 SEK which is quite expensive compared to the second alternative. By calculating the CE index now we have an unequivocal measure to choose an alternative. The results imply that although the first alternative has potential to reduce the risk much better but the expensive cost of it reduces the cost-effectiveness significantly. CE indexes for these two alternatives are equipollent. The CE of the second strategy is slightly less than the CE of first one. This implies that we can choose the second alternative as the most effective countermeasure but as the difference between 18389 SEK and 18290 SEK is not significant we can reconsider again about which alternative to choose taking into account other supportive factors also, for instance, risk tolerance of organization or mitigation covering cost compared with total budget. If the mitigation cost of the second alternative is 5000 SEK instead of 2000 SEK and other numbers are the same then we have $CE_1 = 18389\ SEK$ and $CE_2 = 21290\ SEK$. In this case we have convincing difference between these two values so we can choose the first alternative.

If we visualize the mitigation alternatives by cumulative density function (S-curve), we can see the corresponding curves and compare (Figure 8) [6]. The more left the curve is the lower the expectation of losses is and the flatter the curve is the greater the dispersion of the distribution is. As it can be seen in our example the alternative one (red curve) is the best alternative according to our established criteria.

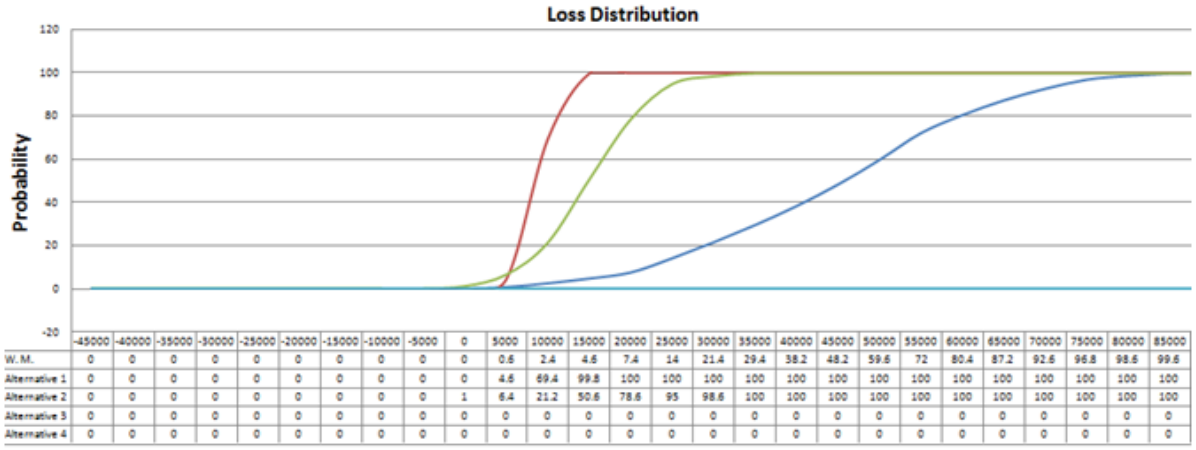

Figure 8: S-curve representation of mitigation alternatives

Before calculating the CE for any risk it is important to ponder about the loss distribution, skewness effect on loss distribution and thus re-consider about the weight of *most likely* value discussed in detail in subsection "Skewness effect on mean value". If the risk is an "either-or" type then evaluation could be done by using the *perceptive method* for avoiding erroneous results. In the next section we elaborate the controlling and monitoring activities of risk volatility, mitigation performance and status.

3.7. Risk Monitoring and Controling

Risk management iteration without controlling and monitoring is like you, when practicing in front of your mirror on how to ask your girlfriend to marry you trying to reduce the chance of rejection and at the same time you do not pay attention to your phone which is ringing and a message from her arrives saying "I want to break you up…. "

Anonymous

The successive action after response plan and mitigation is the monitor and control. This section refers to monitoring and controlling phase which is ongoing unless the mitigation strategy is not completed and can make the difference between successful or failed risk management iteration. We start this section by discussing the importance of control and monitor with respect to the uncertainty parameters of a risk and the monitor of the selected mitigation strategies. Continuing we outline the control and monitor towards financial IT projects, we discuss how Ericsson applies this activity and we cite our solution broken down into simple steps by providing real life scenarios.

A general overview of this activity is that the external environment of risks is tracked and the effectiveness of the risk management iteration is evaluated through the project life cycle. We basically monitor and control the life cycle of the risk and the mitigation strategy applied on it till the time when we have dealt with the risk successfully. In our case that we have to deal with a financial IT project, the monitor and control activity is vital as it is iterative and sometimes the characteristics of the adverse event are unexpected. Iterative and unexpected events in the internal and mostly in the external environment of the financial IT project can affect the characteristics of the risks and our approach to deal with them.

The purpose of monitoring and controlling is to examine the behavior of the hazardous event due to volatility of the uncertainty parameters and to keep track of the successful completion of the mitigation action. *Volatility* in risk management is a quality which describes how frequently the uncertainty parameters of hazardous situation change.

The risk control and monitor phase has to be applied for every single risk regardless its characteristics and chosen mitigation activities. For instance in case of risk acceptance or transfer we might not perform any active response for mitigation but still we have to keep an eye on the behavior of the risk. Uncertain events that might happen to the internal or external environment

of the organization or the project might possibly influence the risk's volatility and therefore we might have to change plans and considerations.

Volatility becomes extremely important when we have to deal with risk in financial IT projects. A financial IT project is always depended on the stock and capital markets as well as on the currency exchange. In this financial environment changes can be made almost every minute and can determine the success or failure of the service. If we do not track these changes then we have an identified and evaluated risk that possibly within two weeks will have different characteristics and different impact and/or loss than the one we expected initially.

As we discussed at the problem domain section the current risk management iteration at Ericsson, does not apply a standard approach for monitoring and controlling the volatility and mitigation strategies for the identified risks. Usually Ericsson performs the monitoring and controlling phase through emails or phone conversations between the project managers and the assigned persons who are responsible for mitigating the risks. This process is based on experience and it does not fulfill the Ericsson needs. In addition the current method can lead to misunderstandings, omissions and not accurate reporting. Important information might be lost during the communication and also different stakeholders might interpret them in different ways.

Even if we have identified a risk clearly and we have analyzed it with accuracy, the whole iteration is incomplete if we are not able to monitor and control the risk's life cycle. In order to perform successful monitor and control activity we must track and report some specific information. Information such as the mitigation performance, the mitigation status and the responsible persons must be clearly identified and reported. On the one hand we update every change that influences the risk and the mitigation activities and on the other hand all the relevant information is stored in a unique repository and they are retrieved effectively without possible losses through indirect communication. All the stakeholders involved in the risk management iteration have common view and understanding of every new action and activity related to risks.

After examination and focusing on the most important aspects of the hazardous events, we have conceptualized the following steps in order to follow the monitor and control phase. Using as example the risks that we have discussed in the identification section we cite the steps of control and monitor conformable those two risks.

Step 1: Report mitigation strategy

Having all the identified risks along with the additional information (country, risk category and partner type) about them via the identification phase we report the chosen mitigation strategy for each risk individually. The available choices as we described in the response planning phase are:

- Acceptance
- Avoidance
- Mitigation

- Reduction
- Transfer
- Share with partner
- Overlook

As we mentioned in the previous section Ericsson applies risk mitigation for Risk1 trying to prevent the failure of transaction. For Risk2 Ericsson comes to agreement to transfer the risk as mitigation strategy and therefore the financial institute is responsible to deal with it. But nevertheless Ericsson has to be informed about the mitigation performance and the volatility level of Risk2 in order to keep track of it. As we have discussed in the response plan section, whichever of the mitigation strategy is applied and even if it is risk transfer, it has to be reported in order to be monitored. Therefore the financial institution informs Ericsson in every control and monitor iteration about the mitigation performance and risk volatility.

Step 2: Set start and finish date for mitigation and assign responsible person

During this step we set the planned start and finished date of the mitigation activity and we designate who is responsible for the performance and control of it. Therefore we can expect when we deal with the risk and also to whom to talk to in case of emergency.

In the case of Risk1 for instance Ericsson specifies that the risk mitigation will have duration of five weeks and Mr. John Brown is responsible for the successful completion. On Risk2 the financial institution informs Ericsson that the mitigation activity will last two weeks. The risk will be avoided and Mr. John Walkers is responsible to eliminate the risky elements.

Step 3: Track volatility

The risk volatility is reported and controlled in this step. After examination we have realized that it is more effective to describe volatility using simple qualitative level of specification. Therefore we divide the volatility level in three categories (In UniRisk we attach a specific colour to each one of the available choices).

- **Stable:** Informs us that the internal and external factors that influence the risk are stable. The conditions remain the same and therefore the planned actions do fulfil its final purpose. The stable level is presented with green colour and indicates that we continue as we have planned.

- **Moderate:** Specifies that the parameters of hazardous situation change but not as much that we have to change our plans. Nonetheless the moderate level indicates that we have to examine the risk's environment more intensively. The internal and external environment of the risk has changed and we have to be careful. The yellow colour of the moderate level indicates a "stand by" mode.

- **Highly Volatile:** This level is presented with red colour and is the warning that the risk situation has been changed dramatically. Therefore we have to review our estimations of probability and loss, choose another mitigation alternative or plan a different mitigation strategy.

In our example during the last monitor and control activity Ericsson has reported that the volatility of Risk1 is stable because the service provider operation has not been influenced and is the expected. On the other hand Risk2 is reported from the financial institute that has become moderate due to the unstable exchange rate variation between YEN and GBP. Nevertheless as we saw in the previous section the financial institution has decided to avoid this risk and therefore the volatility is not so important any more as the risky elements have been removed.

Step 4: Report mitigation activity performance

Mitigation activity performance shows quantitatively how completely is applied the established countermeasure to mitigate the risk in terms of percentages of overall effort. It is an easy way to have all stakeholders informed about how we progress with mitigation. The performance is presented with percentage and can have the values 0%, 25%, 50%, 75% and 100%. Its value along with a progress bar provides us the current completion state of the mitigation activity. Value that equals to 0% indicates that risk is in its identification phase and a mitigation strategy has not been planned or started yet. Value of 50% indicates that we are in the half way and 100% that the mitigation is completed successfully.

The risk mitigation performance for Risk1 is reported to be 25% which means that Ericsson has already started the mitigation process. On the other hand the mitigation performance of Risk2 is 100% which means that the financial institution has completely avoided the risk.

Step 5: Monitor mitigation status

This step indicates the status of the mitigation activity. Three words with the appropriate colour background can be presented and indicate the mitigation status. In UniRisk the status report is automatically connected to the mitigation performance. When the mitigation performance changes according to the given criteria, the status changes as well. Therefore the three status values are:

- **Open:** Refers to the mitigation activity that has not been started yet and the performance of it is 0%. This choice is displayed with red colour.
- **In progress:** Refers to the mitigation activities that have already started and their performance is between 0.1% and 99, 9%. The colour of this choice is yellow.
- **Closed:** Refers to a completed mitigation activity and therefore we have performance of 100%. This value is presented with green colour.

Based on the reported mitigation performance, the mitigation status for Risk1 is “In progress” as Ericsson has already started mitigating the risk and for Risk2 is “Closed”, because the financial institute has applied the risk avoidance strategy and has avoided the risk completely.

Step 6: Update Review

We report the date of the last checklist review and we describe briefly the last activity that has been performed during the monitor and control process.

For both our risks the last review update has been done in the 25th of April and both Ericsson and the financial institute reported all the last updates along with a description of the last mitigation action.

Step 7: Report history of mitigation activity

This step can provide guidance for the mitigation strategy and the monitoring of it. In case that we have faced the same or similar risk in the past and we have applied the same mitigation strategy to deal with it, we report our experience and lessons learnt in order to perform the mitigation strategy this time without facing issues that we probably have faced in the past.

As Ericsson Money Services is the first financial IT project of Ericsson there is no mitigation activity history for Risk1. On the other hand the financial institute has significant experience in risks of type Risk2 and the lessons learnt from the past are used as guidance to deal with this case.

Concluding this section we have to mention that in order to have successful control and monitor activity we are required to do frequent updates and reports of the risk’s uncertainty parameters and the performance of the mitigation strategies that are applied to every risk individually. The co-ordination of actions, the accurate estimation of time to deal with the risk and the proper mitigation performance reporting among the responsible persons of each mitigation strategy is vital with respect to risk dependencies in project and program level as we discuss in section “Risk Dependencies”.

In the next section we focus on the risk overlook mitigation strategy that we have mentioned in the “Risk Response Plan” section, in order to deal with inceptive events of risk. The track and monitoring of inceptive events of risk is connected to the overall control and monitor phase of risk management iteration.

3.8. Inceptive Events of Risks

"An elegant solution for keeping track of reality"
Ariande, Inception (2010)

In the previous section we have described the control and monitor activities as we propose to be applied in the risk management iterations. As we have mentioned there are seven different categories of risk mitigation activities. One of them is the risk overlook. Risk overlook is applied to inceptive events of risk. An inceptive event of risk refers to an event that has been identified to be potentially hazardous, but we still examine specific internal and/or external factors that influence it in order to start dealing with it. Each internal and external factor that influences the particular risk is described as an event scenario. Once an uncertain factor becomes true, the event(s) in the scenario are triggered and therefore risk evaluation, analysis and mitigation has to be performed. In other words a potential risk is identified and we wait for a specific condition to become true in order to start dealing with this particular risk.

During most of the risk management iterations inceptive events of risk are not included in the used checklists. Mostly they are not reported or documented and the different project or risk managers have them at the back of their mind. Therefore the inceptive events are difficult to be communicated, examined and tracked. For instance EURO is very unstable due to the financial crisis in the Euro zone. The likelihood of the EURO not to exist as a currency is significantly less due to the disciplinary measures that European Union has applied. The elimination of EURO as currency seems not to be highly probable but nevertheless is an inceptive event of risks, henceforth we identify it along with a scenario that pulls the trigger for a risk which becomes critical and requires examination.

In this section the "EURO" scenario is used as guidance and we outline our approach on how inceptive events of risk should be reported and monitored. This scenario of inceptive event of risk is communicated between Ericsson and the financial institute as it can influence both the Ericsson Money Services normal operation and have financial impact as well. Using simple steps in this section we outline the phases to be followed in order to perform this activity.

Step 1: Specify source of inceptive event of risk

As we also do in the risk identification phase we specify the source of the risk by determining the risk category, country, source and partner type along with the description of the inceptive event of risk. In case of the EURO inceptive event of risk Ericsson specifies the characteristics of the inceptive event as presented below:

Category: Financial and accounting

Country type: Euro zone countries

Source: Financial crisis

Partner Type: Bank

Step 2: Inceptive event description

A description of the event is provided in this step. In our scenario Ericsson defines the inceptive event of risk as:

"There is a possible elimination of EURO as currency in the Euro zone countries due to the financial crisis. Therefore Ericsson Money Services has to be aware that EURO might not be used as currency in the money transactions."

Step 3: Decide action

Action is similar to mitigation strategy in case of inceptive events of risk. In this case we have two kinds of actions against the inceptive events of risk that is "act" or "overlook" the spawned hazardous situation. As we have described in the introduction of this section, for the inceptive events of risk we apply the risk overlook strategy initially and by default so we just monitor the condition of the inceptive event. Once the inceptive event generates risks then the mitigation strategy changes to "act" and we identify it as a risk and all the risk management iteration steps have to be performed to deal with it. In our case Ericsson leaves the default choice of action which is risk overlook.

Step 4: Define trigger event

This step can be characterized as the most momentous during this phase. Here is where the trigger event/scenario is specified. In case of this scenario becomes true we have to evaluate our risk, which emanates from the inceptive event a real risk that we need to deal with. Ericsson defines the trigger event as:

"One of the countries that belong to Euro zone cannot get bailout package to fulfill its liabilities in terms of bonds to the capital markets and therefore it will be a credit event and by default the whole Euro zone will collapse. We must pay special attention to the financial situation in Greece, Portugal and Spain "

Step 5: Report tendency of trigger event

Tendency provides us with the information about the trigger event and is the precursor to the status of the inceptive event of risk. The trigger event is examined in order to track its tendency and in sequence the status of the inceptive event of risk. The tendency is determined using arrows that express how the trigger event tends to be. The arrows can point three directions; up, horizontal and down.

Positive: In this case the conditions that influence the trigger event tend to become more and more encouraging. This means that the trigger event has even less possibility to become true.

The positive tendency is presented as a green arrow pointing up. A positive event for Ericsson is:

"Currently there is no country in the Euro zone that is not able to fulfill its liabilities".

Stable: This value indicates that the trigger event does not tend to get better or worse. The condition remains the same as it was when we identified the trigger event. The arrow has yellow colour and a horizontal direction which represents the stability of the trigger event.

"The financial condition in Greece, Portugal and Spain remains the same".

Negative: When this value is presented it means that the trigger event is prone to worsening and it influences also the inceptive event of risk status. The negativity is presented with a red arrow that is pointing down. A negative tendency can be described by Ericsson as:

Apart from Greece, Portugal and Spain after the latest reports from the European Commission, Italy is also in financial instability".

Step 6: Report status of inceptive risk event

The status report refers to the inceptive event of risk that is described in step two. We monitor and track the status of the given inceptive event of risk in order to update the latest condition of it. We propose three values for status that are expressed as traffic lights colors:

Green: We examine the inceptive event of risk and we see that the condition of it is unchanged and thus positive, which means that the internal and external factors are in a positive situation. In the Ericsson case this means that:

"The stock and capital markets in the Euro zone are in positive trend so the countries that are in danger seem to be able to pay their liabilities."

Yellow: After examination of the inceptive event of risk we see that the condition become worse than before and therefore Ericsson might soon have to deal with the inceptive event as a real risk.

"The capital and stock markets are discouraging and the credit default swaps of Greece are dramatically high, which means that is quite possible for Greece not to be able to pay its liabilities."

Red: If this value appears then it means that the inceptive event become a risk that we have to deal with. The red status is close to match the inceptive event of risk description which means that what we have expected has high probability to happen. The trigger event is activated and therefore the inceptive event of risk became a real risk that Ericsson has to evaluate, examine and mitigate.

“Greece is not able to bail out its liabilities. The country defaults, thus the whole Euro zone is close to collapse and the entire Euro zone countries will use again their pre euro currencies. “

Step 7: Report Update:

In this step we simply report the last date of tracking the status of the inceptive risk event and the tendency of the trigger event.

The two core steps of this activity are five and six which are connected and interacted with each other. The status of the risk inceptive event is determined by the tendency of the trigger event. Nine combinations of status and tendency are possible. The best scenario is “Green” status with “Positive” tendency and in this case the inceptive event of risk is the least likely to become risk. The worst case is “Red” status with “Negative” tendency which means that the likelihood of the inceptive event to originate an active risk is the highest possible. When we meet “Red” status with “Negative” tendency then the change of action is enabled and turns from “risk overlook” to “act”. The philosophy behind this method is that in the worst case, the inceptive event of risk becomes automatically an identified specific risk to be evaluated, analyzed and mitigated. All the rest seven possibly cases are leaved to the project and risk managers to judge whether the inceptive event of risk has to be further examined and monitored or to be accepted and ignored.

Performing the inceptive events of risk identification and monitor we conclude complete and thorough risk management iteration. Besides analysis and controlling of the already known risks we have now taken action for inceptive events of risks that have the character of potential risks. Our sleeps can become more peaceful from now on.

3.9. Risk Iteration Report

“Initial reports are encouraging. In the end of the day, it's going to be deeds, not words that matter.”
Stephen Hadley

After completion of the phases that are described previously, in this section the project risk management iteration is close to termination. The final phase that completes full project risk management iteration is a summarized final report that is presented and distributed among all the participants of the iteration. The essence of this phase is the comprehensive information for the participants about the results of the iteration and the participants’ self-examination on the whole process and preparation for the next project risk management iteration. The final iteration report has the serviceableness as the input for the coming iterations. The duration of producing the report using UniRisk is immediate. Nevertheless specific disagreements, concerns and comments on the reported results must be written down and reported. The duration of this process depends on the participants and the specific deadlines that the risk iteration facilitator sets.

In this report the most important information collected during all the phases of the risk management iteration are presented, moreover, the following outputs are summarized:

- A complete list of the identified risks
- The risk value without mitigation for each risk individually
- The risk value and cost effectiveness of all the mitigation alternatives for each risk individually
- The best alternative along with its cost effectiveness for each risk is highlighted
- The responsible person for each mitigation activity
- Enrolment of the participants according to their experience where they can reason whether the chosen mitigation alternative seems to fit its purpose.
- Assumptions and concerns about the iteration and the outcome of it.

The results above are documented and presented using a template that consists of standard sections. In addition to the output described above there is some general information about the project and the risk management iteration that is presented as well in the report such as:

- Date of the project risk management iteration
- The project risk management iteration ID
- Customers ID and name
- The operational region of the project
- List of facilitator and participants
- The money currency of the values used during the evaluation
- A small overview of the taken decisions
- Feedback on the effectiveness of the iteration

In case of projects that run under the same program and enable correlated risks, the report contains all the information presented above plus the report of the project representatives on how successfully they completed the beforehand discussed and assigned or commissioned tasks concerning correlated projects or risks.

Through this section (Proposed Solution) we have presented in details all the phases of the project risk management iteration, starting from the identification till the final report and the presentation of the results. In the coming section we discuss the risk dependencies technique and how it can be integrated to the project risk management iteration.

3.10. Risk Dependencies

"Never make solid plans when you depend on others, True Story"
Anonymous

In big organizations such as Ericsson they usually have several projects implementing different parts of one product. Mostly when different projects move towards the same goal they may have one coordinating center called program. *The program is an organizational structure which aims to create a business value and includes several interrelated projects.* In such organizations the risk management process becomes a complicated task and it is sometimes hard to make optimal decisions for the mitigation activities and control. This section is focused on introducing a simple and easy-to-use instruction for managing risks in program context.

The risk dependency or just a dependency in a program is the interrelation of two or more projects due to an emerged risk in any of those projects. Dependency level of two projects indicates the relative severeness of the impact on one project when the second project is suffering from a setback [13]. The different types of projects dependencies because of risks are:

- A risk that is arisen in one project can be arisen in another project also (probably with different severeness) thus affecting whole program.
- In several projects while performing risk mitigation the same risk can be mitigated multiple times because of unawareness and lack of communication among projects.
- One risk that is identified in one project could be latent in another project. This case particularly is important when the first project decides to accept the risk whereas it has significantly greater effect on the later one and mitigation is vital.
- Two or more risks emerged in several projects are correlated thus raising the overall impact.

Whenever an organization tries to establish a way of communication and report between projects in a program it will confront a complicated task:

- How to organize communication process effectively and in a simple way?
- What information must be transferred across projects while identifying risks?
- How intensively exchange the necessary information across the projects?
- What is the next step when the information is provided?
- What if we have different software development methodologies?
- After all is the specified way of communication effective and not time consuming?

The task becomes more complicated when it comes to financial IT projects in case of which there are external partners with whom negotiations, risk sharing activities and contracts can be established. Usually not only program but also projects can perform some independent activities such as negotiations and contracts. In this case we have all the possible interactions due to

emerged adverse event. Figure 9 is an example of how several projects can be dependent on program, external partners or to each other. Blue arrows show the possible dependencies between units due to emerged risks. The interactions between partners are considered to have comparably little effect on the program.

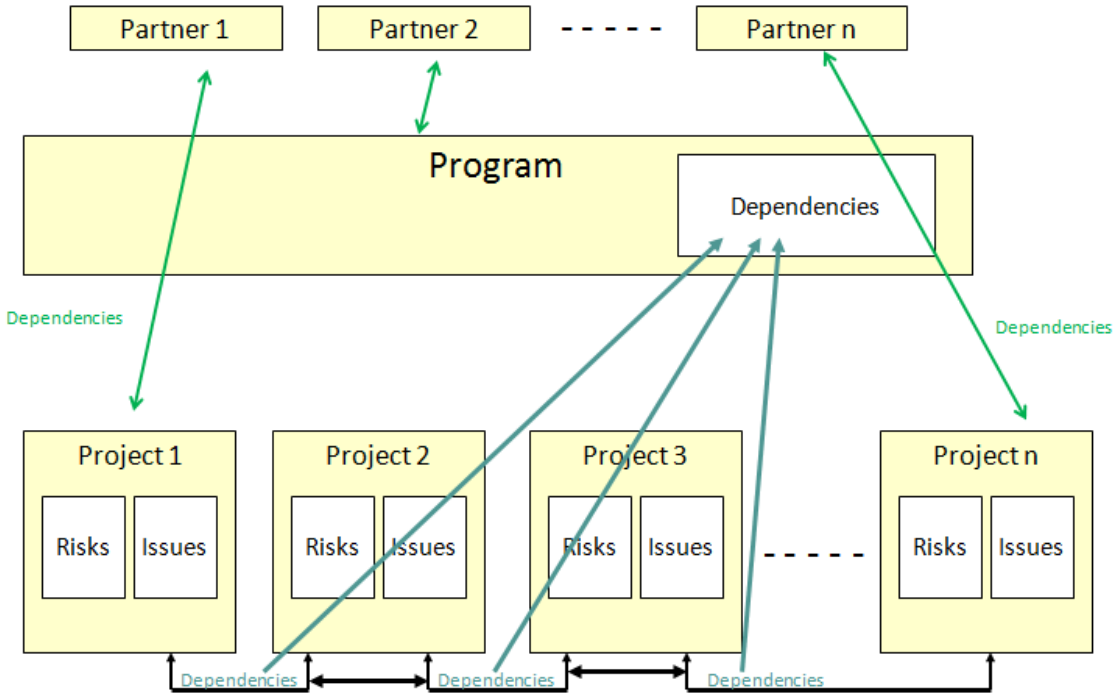

Figure 9: Risks dependencies among projects, program and partners

If we assume that all projects follow the Waterfall model we can insist that the risk management activities are carried on with the same intensiveness say in every two week. This claim is confirmed by Ericsson where the PROPS models have established definite schedule for risk analysis and mitigation. Whenever we have firmly established schedule for risk management activities in every project and thus in the program we can schedule the time in a way that risk analysis and assessment take place in the same day for all the projects. During risk assessment in program level all the projects have their representatives. The only task in this case is to discuss and decide who the responsible is for a certain risk and in the next session or meeting before beginning the new identification and assessment the representatives can report about mitigation status of a risk which was assigned in previous session. The view is different when we have different development methodologies. While in Waterfall model there is an established schedule for risk analysis, the projects following Agile processes and particularly Scrum do not have any routine for performing risk management activities. Instead it is done as the team finds convenient or relevant to do (usually more intensively then in Waterfall based processes). When we address to create a method for communicating and settling issues of dependencies we must take into

account the fact that we cannot oblige projects to do untimely assessment to provide the necessary results. Examining all these issues and facts we establish the following steps and information registering mechanisms to provide a simple and effectual procedure of controlling risk dependencies in program context:

Step one: Setting private risk management schedule

In every project there is established schedule (depending on the project development methodology the time frequency of analysis and mitigation can differ) of doing risk analysis. Frequency of identification and analysis process and estimation methods does not affect herein described procedure.

Step two: Independent assessment of risks

The risk management responsible person (risk manager, project manager, scrum master…) with the analysis team fulfils risk identification and loss estimation for every risk in the project context. The mitigation activity, cost and later activities must not be specified yet.

Step three: Report to program level

For the purpose of risk report from projects to program level there must be created an email account wherein from the projects the necessary information must be sent and on which the program manager can have control (In some cases a partner organization can be provided with this email address to provide any common risk that they may have). The program manager must register the risk description and assessed impact in the risk management tool. The risks that have no direct impact to other projects must not be provided otherwise they will overload the dependency evaluation process. This kind of risks can be discussed orally in reporting process and program manager will decide to register those or not. If it is quite clear that the risk is purely concerning to only own project, then the project manager does not need to report it at all. The program manager must check the email in every week*.

Step four: Registering the necessary information in the checklist

The program manager with the risk analysis team specifies the time and interval for the risk analysis activity in program level. During the program's risk identification process the risk facilitator with the other participants have all the registered risks by weekly checking of the email.

---

*We found that when there is a scrum following project one week can be the best choice but depending on the stability level of projects, their risk tolerance, external effects and other number of reasons the program manager with the analysis team can decide how frequently to check email and update the information.

Based on this information they make the decision on which risks of the projects must go to the program level for mitigation, which ones must be mitigated in the same project, which should be mitigated in other/several projects at the same time (communication between those projects can be established in very short and informative way, succinct oral negotiation and agreement) and which must be negotiated with a partner organization or shared. Having all the reports from all projects the risk management team should also discuss which risks are correlated. All these information must be registered in UniRisk. The information that must be filled in for a risk in the tool is:

- The reported risk description
- In which project the risk has been identified
- The dependency level of other projects from the one where the risk is identified, expressed with three qualitative indicators: *Low, moderate* and *high*
- Risk exposure values for all the projects that have this risk and for the program
- In which project it should be mitigated or with which partner must be shared.
- The active mitigation cost
- The risk number that has correlation with it.
- The status of the mitigation performance

Step five: Completion of assigned tasks

After having all the information about a risk (which project can be affected, in which project it must be mitigated, dependencies of projects according to that risk, mitigation cost and correlation with other risks), the project and program managers complete their risk management activities in their projects/program level. In the coming report project managers inform about how they have completed the agreed assignments or they can be informed if the risk is closed already in other projects or program.

Step six: Iteration end and inception

The iteration cycle finishes when program risk analysis activity is done. Then the iteration starts again. During the iteration a project manager may report several times or not at all. It depends on the period of the risk analysis activity and the software development methodology. The information mentioned in step four that must be filled in UniRisk is not obligatory. The program manager may decide not to fill the mitigation cost or a project manager may decide not to estimate the risk relative exposure. The obligatory fields that must be marked are: which project the risk can affect (*dependency level*) and who the responsible is for the mitigation. Specifying mitigation status also will be helpful. The figure below visualizes this six-step procedure.

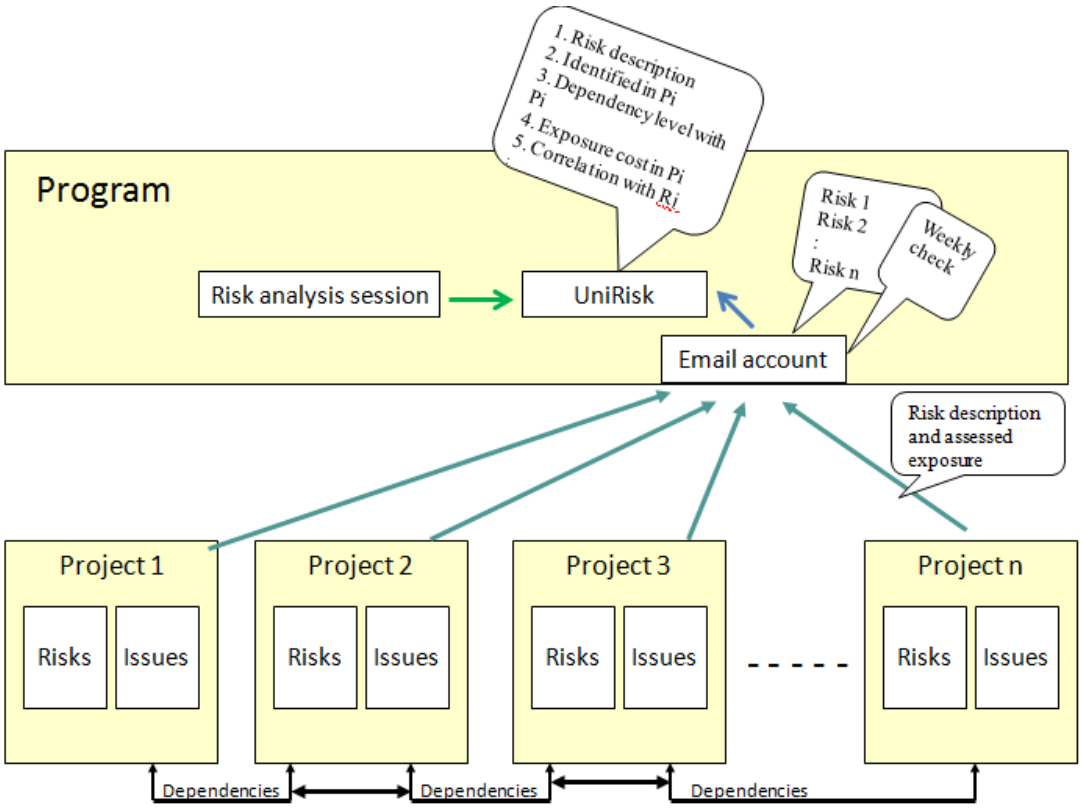

Figure 10: Risks dependencies method visualized

The usage of the procedure does not allow the user to calculate the correlation level of risks or how much the risk impact on one project affects to other projects but it allows to communicate the already identified risks in program context and to manage those risks, their interrelation and correlation effectively.

As we have shown in the previous sections the first eight steps of risk management do not need to have any beforehand specified frequency. In different projects and with different development methodologies the frequency of risk analysis sessions is different. The first eight steps of the risk management iteration can be performed independently according to specific characteristics of each project and based on the software development methodology that is applied. The identification, estimation, analysis and mitigation activities cannot be affected by the software development methodology as they do not require beforehand specified timeframe. Conversely when it comes to dependencies, different projects have different frequency of risk management session, nevertheless, as we have presented earlier in this section the project risk facilitators do not need to consider about other projects' risk management activities. Instead they must send the necessary information to the program risk facilitator whenever they have new identified risks. It is the program risk facilitator who needs to check the sent information every two weeks obligatory. This last activity is carried out in program level independently from any software development methodology in any project, hence is not influenced by any project characteristics.

4. Evaluation

"True genius resides in the capacity for evaluation of uncertain, hazardous, and conflicting information."
Winston Churchill

Aiming to secure the effectiveness and accuracy of the results that our work brought to light and also test the usability of UniRisk we have had to evaluate our work across real life scenarios. UniRisk was built in order to serve professionals in risk management and also beginners in the field. Therefore the evaluation has focused on these two categories of people and it consists of two parts each one of which has aimed to provide a different result and feedback covering different aspects of our results.

The first part of evaluation is to test UniRisk is real projects that Ericsson launch or will launch in the future. During this phase the final version of UniRisk that we have delivered to Ericsson will be used as an option for completing the risk management iterations both in project and program level. Ericsson stakeholders will apply our approach through the implemented tool in order to perform risk management for the planned projects. Due to time constraints of delivering our final thesis and also to reorganization of Ericsson units the current period, this part of evaluation will come with a delay and after the completion of the thesis. Nevertheless the feedback that Ericsson will give is of high importance as it represents the opinion of experts on our work.

The second part was the UniRisk testing by our university colleagues that have limited knowledge in risk management. This process was carried out by giving some simple daily life scenarios to them and asking to evaluate the uncertain situations by providing their estimations. The results given by UniRisk were matching with the expectations of our colleagues. During this phase of evaluation we focused intensively to the perceptive method aiming to prove that the choice of available words makes the selection of likelihood to the uncertain events easy for the user. In addition during this part we received consultation and we had discussions with professors form the literature and language department of the University of Gothenburg and with Prof. Steen Lichtenberg owner of Lichtenberg and Partners management consulting company and former professor of Project Management & Project Economy at the Technical University of Denmark. Indeed the feedback that we got from our colleagues was very positive as they found our method understandable and easy to use. Moreover Prof Lichtenberg showed interest to our approach and he mentioned that in the past during forums and conventions of risk management they have tried to create such an approach for "either-or types" of risks.

Concluding the evaluation of our work we have to present our results and submit the final document to our examiner. The final oral presentation and opposition will give us the opportunity to make clear if we finally met the requirements of the university and the aims and purpose of the master thesis from an academic perspective.

5. Discussion

"Discussion in America means dissent."
James Thurber

Whatever set of rules or principles we establish while performing an activity we always need to ponder about how the vagueness of these principles will affect the pursued results. As a financial IT project risk management approach the set of principles and mechanisms that we propose does not require much administrative time and effort. The main reason is that it does not suggest collecting all the possible information that can enlighten uncertainties while developing financial project. For instance we purposely avoid discussing all the constitutional issues of different countries or different financial institutions which might prevent establishing contract with Ericsson Money Services. Instead we propose to register the country or contracting partner type and examine specific issues only. Later we can use the identified issues as new information for new contracts. Likewise we specify how to deal with projects dependencies among a program by specifying an effective and easy-to-use method for keeping track of the common risks among the projects and their correlations. Nevertheless we do not calculate how much the correlation of two risks quantitatively is or identify if it is negative or positive correlation. Usually in financial institutions it is pivotal task to identify the correlated risks but when it comes to IT projects it is not that important to do full scale analysis and it is let up to the project managers to understand and manage details relying on their experience and predictions. Conversely we pay much attention to assessing the risk exposure quantitatively because this is the pivotal action in risk management and requires as much precision as possible to understand how to select the right countermeasure and apply it. But at the same time whichever method is applied for risk assessment it must be not only effective in terms of having sufficient enough results but also simple to be applicable and available not only for risk managers but also any experts in the software engineering field.

The triple estimation formula as we have discussed is proven to be more effective and trustworthy despite the arisen issues because of skewness effect of loss distribution. Analysis shows that it is not possible to have a standard formula or approach to apply and bypass the skewness effect on risk assessment but it is possible to know some simple rules and be orientated according to these rules to reduce maximally the errors. Alternatively we suggest a new method to tackle the "either-or" type of risks which are burden for triple estimation approach. Although the perceptive method, which aims to deal with "either-or" type of risks, seems to be easy and relies on human perception of reality by using natural language, it is not applied on assessing real industry risks and we suggest that it can be improved in its evolution immensely.

The main hindrance of creating a competent method for financial IT project risk management is that there is not a similar study to examine and understand the key factors to concentrate on detail examination. The risk management approaches that are applied in banking systems or safety critical systems are totally different and either are not applicable or take too much

administrative time and effort to justify its application. For instance in banking systems they usually collect vast amount of statistical data and might do regression analyses or in safety critical systems such as NASA operations they usually concentrate on the human factor of error and regard whole system as a homo-technological system.

The mathematical formulas that we suggest are reasoned based on both life time experience and mathematically provable arguments. Conversely the other steps of herein risk management procedure rely on critical thinking and have framed on the ground of Ericsson Money Services operations.

6. Conclusion

A conclusion is the place where you get tired of thinking.
Arthur Bloch

As we stated at the purpose and result sections at the beginning of the document the expected results of our work were specified at an early stage of the thesis. Nevertheless during the process of completing the thesis we have examined a variety of aspects and provided solutions to issues that can possibly rise during the project risk management iteration and were not specified at the beginning of our work. This section provides a compact outline of our findings and results and it is divided in two sub sections which are the theory behind the functionality of UniRisk and the effective application of UniRisk during the project risk management iteration for financial IT projects and IT projects in general.

Our approach on how to perform project risk management consists of eight main steps plus a ninth one in case that we have projects that run under the same program and risk dependencies and correlations has to be identified. A brief summary of our findings on each step of project risk management is outlined below.

- **Project risk management iteration**

The key facilitator and participants are identified and informed about the purpose of the process, the expected result and the role that each one will have during the process. Moreover, the frequency of the iteration during the life cycle of the project has to be determined.

- **Risk identification**

The potential risks are identified and registered based on specific properties of them. The source and type of these specific properties we have clearly specified. In addition we have provided guidance on how to register and examine potential risks according these properties.

- **Qualitative assessment**

Our research and solution approach have shown that the qualitative assessment of risks as it is applied by Ericsson is only effective for the prioritization of risks and cannot give trustworthy results of qualitative attributes of risks. In addition we have outlined the weaknesses of this method and we proposed our approach on how to use it efficiently.

- **Quantitative assessment**

The skewness of loss distribution as the main hindrance of applying triple estimation method, while assessing risks quantitatively is discussed and evaluated. We also have determined the risk value and cost-effectiveness of the mitigation alternative unequivocally.

- **Perceptive method**

Based on human perception of the reality and its expression by natural language we have developed a method to deal with "either-or" type of risks. We have discussed the purpose of this method, the analysis behind it and the special cases where its application most likely can bring more accurate results than the traditional methods.

- **Risk response planning**

We have provided our approach on how to specify the risk response planning and have identified a set of possible response plans that cover all the aspects of response types to risks along with simple scenarios in order to make clear in which cases each one is applicable.

- **Analysis and countermeasure selection**

We have achieved a detailed presentation of the different mitigation alternatives to a risk with respect to the mitigation cost, the risk value and the cost-effectiveness. In UniRisk we managed to present all the possible alternatives for a single risk, display comparable probability-loss distribution curves and highlight the best alternative along with the cost-effectiveness of it.

- **Risk monitoring and controlling**

We have specified all the needed indicators in order to keep track of the volatility of risks and also control the performance of the planned mitigation activities. In UniRisk we have implemented this process to be performed simply and automatically using standard notation.

- **Inceptive events of risks**

This concept relies on registering the inceptive suspicious events which might become later risks in order to control and monitor potential risky situations that do not require any specific actions.

Dependent on some specific conditions that influence these risky situations we can make decision to regard these events as risks or follow the possible variations. Through UniRisk we provide a simple way to keep track and control such situations.

- **Risk iteration report**

At the end of each project risk management iteration a final report has to be delivered to all the participants. We have highlighted which information is needed to be documented and the purpose of the report for the coming iterations.

- **Risk dependencies**

We have created a method on how to identify risk dependencies and correlated risks arisen in projects that are interconnected to each other's and run under the same program. This method is fully integrated to UniRisk in order to save time and have an organized full approach on project risk management.

Final outcome of the analysis and findings of the phases described above is implemented in UniRisk which is a complete tool capable to perform all the necessary activities of project risk management. UniRisk is a user friendly, efficient and automatic checklist tool that is easy to understand, use and modify and refers both to experienced practitioners and beginners in the field. The tool also gives freedom to users to modify, change and examine critically the given results by providing their opinions, concerns and assumptions.

Concluding we have examined the application of project risk management through the software development methodologies and particularly Waterfall PROPS and Agile Scrum. The risk management procedure that we have introduced in this framework is shown to be easily integrable in any financial IT program containing several projects which run according to different development methodologies but on the other hand the management process can be very flexible and be adapted to every different kind of project individually. In addition we have analyzed the critical factors that influence the application of risk management. Therefore we leave an open window on how to specifically apply project risk management which relies on the different goals and needs that different organizations and projects have. Nevertheless risk management is a critical process that has to be mandatory when building and maintaining a product and can determine significantly possible success or failure.

We would like to mention that since the 4th of April 2012, Ericsson Money Services is not longer available due to unknown possibly technical issues. Nevertheless UniRisk is applied to other projects running in the division of M-Commerce of Ericsson.

Reference List

[1] Gokarna Aryal, A.N.V. Rao (2005), Reliability model using truncated skew-Laplace distribution, University of South Florida, USA

[2] Mike Cohn (2009), Succeeding with Agile: Software Development Using Scrum, ISBN-13978-0-321-57936-2, Addison – Wesley, London, UK

[3] Romney B. Duffey, John W. Saull (2008), Managing Risk the Human Element, ISBN: 978-0-470-69976-8, John Wiley & Sons Ltd, United Kingdom

[4] Merran Evans, Nicholas Hasting, Brian Peackock (2006), Statistical Distributions, Monash University, Queensland University of Technology, Australia

[5] Rick Hesse (2000), Distribution: Mathematical Link for Excel, Pepperdine University, USA

[6] Douglas W. Hubbard (2007), How to Measure Anything, Finding the Value of ‘‘Intangibles’’ in Business, ISBN 978-0-470-11012-6, John Wiley & Sons Inc, Canada

[7] Douglas Hubbard (2009), The Failure of Risk Management – Why it’s broken and how to fix it, ISBN 978-0-470-38795-5, John Wiley & Sons, Inc., Hoboken, New Jersey, USA

[8] Philippe Jorion (2007), Value at Risk – The New Benchmarking for Managing Financial Risk, The McGraw-Hill Companies, USA

[9] Steen Lichtenberg (2000), Proactive Management of Uncertainty Using the Successive Principle: A Practical way to Manage Opportunities and Risks**,** Polyteknisk Press Anker Engelunds Vej 1 DK-2800 Lyngby (Denmark)**,** ISBN 87-502-0822-5

[10] Thomas Norman (2010), Risk Analysis and Security Countermeasure Selection, 978-1-4200-7870-1, 2010 by Taylor and Francis Group, LLC, New York, USA

[11] Klara Persson, Jesper Riden (2010), Exponentiated Gumbel Distribution for Estimation of Return Levels of Significant Wave Height, Journal of Environmental Statistics, Sweden

[12] Andre Söderlind (2007), Risk management in IT projects, Master of Science Thesis in Master Degree Programme – International Project Management, Department of Civil and Environmental Engineering, Chalmers University of Technology, Göteborg, Sweden

[13] Kwan Tak Wah (2009), A Risk Management Methodology with Risk Dependencies, Thesis for the Degree of Doctoral in Philosophy, The Hong Kong Polytechnic University

[14] Nassim Nicholas Taleb (2001), Fooled by Randomness, The Hidden Role of Chance in Markets and Life, Texere, New York

[15] Debbie Tesch, Timothy Kloppenborg, Mark Fidick (2007), IT Project Risk Factors: The project management professional perspective, Xavier University, Cincinnati, OH, USA

[16] Brad Touesnard (2004), Software Cost Estimation – SLOC Based Models and the Function Points Model, UNB, University of New Brunswick, Canada

[17] Hans van Vliet (2008), Software Engineering: Principles and Practice – Chapter 1, ISBN: 978-0-470-03146-9, John Wiley & Sons, New York, USA

[18] Project Management Institute (2008), A guide to the project management body of knowledge (PMBOK Guide) – Forth Edition, Pennsylvania, USA

[19] Washington State Department of Transportation (2010), Project Risk Management Guidance for WSDOT Projects, Washington State Department of Transportation Administrative and Engineering Publications, USA

[20] http://www.ericsson.com/news/110608_money_244188810_c (Accessed November 2011 to April 2012)

[21] https://www.ericssonmoney.com/welcome (Accessed November 2011 to April 2012)

[22]http://www.iso.org/iso/iso_catalogue/management_and_leadership_standards/risk_management.htm (Accessed November 2011 to April 2012)