VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

RISK MANAGEMENT SUPPORT SYSTEM

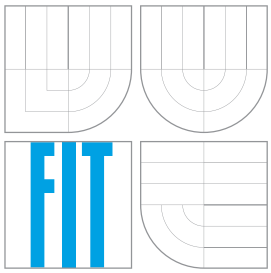
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

JAN KUBÍČEK

BRNO 2010

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

SYSTÉM NA PODPORU ŘÍZENÍ RIZIK

RISK MANAGEMENT SUPPORT SYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — JAN KUBÍČEK
AUTHOR

VEDOUCÍ PRÁCE — doc. RNDr. JITKA KRESLÍKOVÁ, CSc.
SUPERVISOR

BRNO 2010

ZDE VLOZTE ZADANI

Abstrakt

Práce poskytuje teoretický úvod do projektového řízení. V práci je popsán současný přístup k řízení projektů jako kombinace několika procesů. Procesu řízení rizik je v práci věnována větší pozornost. V práci je také diskutováno několik přístupů k řízení rizik, která jsou v současnosti považována za nejlepší.

V práci je navržen zcela nový přístup k řízení rizik, který kombinuje znalosti z oblasti získávání znalostí z databází s řízením rizik. Současně je přístup získávání znalostí z databází použit na vytvoření orientačních hodnot při kvantitativní analýze rizik. Navržený přístup byl úspěšně implementován a otestován. Testy ukázaly, že tento přístup je vhodný pro hledání rizik, na které uživatel zapomněl. Tento přístup je bohužel nepříliš vhodný pro navrhování orientačních hodnot při kvantitativní analýze.

Abstract

The work provides theoretical base of project management. It describes the current approach to project management as a combination of multiple processes. The process of risk management is described with special care. It also discuss some of the different approaches to risk management.

The work suggests new way of handling risk management, that combines risk management and data mining. Data mining approach is also used to mine quantitative risk values. This approach was successfully implemented and tested. Tests showed that this approach is very useful for ommited risk identification. Unfortunetaly it is also not recomendable for minig quantitative risk values.

Klíčová slova

Projektové řízení, řízení rizik, dolování dat, podpůrný systém, identifikace rizik, kvalitativní analýza, kvantitativní analýza

Keywords

Project management, risk management, data mining, support system, risk identification, qualitative analysis, quantitative analysis

Citace

Jan Kubíček: Risk Management Support System, diplomová práce, Brno, FIT VUT v Brně, 2010

Risk Management Support System

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením paní doc. RNDr. Jitky Kreslíkové, CSc.

.....
Jan Kubíček
May 26, 2010

Contents

Chapter 1

Introduction

As project management is today's one of the leading styles in fulfilling goals within companies, it sometimes advances in scope to such measures that the project is no longer manageable without software support. Risk management is an integral part of project management. The aim of the work is to asses a new approach to help project managers performing risk management.

In the following chapters we will first go through the whole process of project management to better understand the context of risk management. As project management is not precisely defined, we will try to adhere to what is called best of practice. There are a few standards of project management, which are recognized all over the world. We will compare some of them. Because the focus of the work is risk management, in the next chapter we will take a closer look at the risk management process. Going in detail through the process we will have a look at current methods. The next chapters provide a description of specification and design of suggested project management support software. Together with the next chapter, which describes implementation aspects of the work, they form the core of the project. The next chapter talks about test done to asses the quality of the proposed approach and discuss results. The last chapter concludes the work with future development prospect.

This master's thesis follows the suggested approach from my semester thesis. The chapters, that are considered as theoretical part of this work (2, 3), as well as parts of chapter that deals with system design (5), were used as results of semester thesis.

Chapter 2

Project Management

Project management is a systematic approach to planning, organizing and managing resources to fulfill goals and objectives of a specific project. There are defined processes through the whole project. Not all processes are always applicable to all project so the standards [3] or [1] are a guide to be followed.

2.1 Knowledge areas

According to [3] there are knowledge areas that each project manager should know. That means he should be aware of all areas and processes during the whole project life. A simple matrix is shown (2.1) to demonstrate the connection between them.

2.2 Initiating process group

Initiating process group stands partially apart of the project when it starts up a brand new project, because it has to start prior to the project (as a project beginning is sometimes considered *Project charter*). But it may as well start a new phase within existing project. Two main goals of Initiating process group according to [3] are to produce *Project charter* and to identify stakeholders. It also considers these two tasks as separate and following each other. Let us have a closer look at these outputs.

2.2.1 Project charter

Considering division of processes according to [3], the process owner of creating a *Project charter* is Project integration management. The inputs are statement of work, business case, contract, risks, enterprise environmental factors and organizational process assets. As stated before it is the formal beginning of the project. It should contain the purpose of the project, high level description of all following processes and budget. If suitable, it should also appoint responsible project manager and sponsor, to whom will be referred as authority for approving the charter.

As can be easily seen, this process is not independent on stakeholders identification. It has to take all possible risks in account and stakeholders are one of the sources of these risks.

Knowledge areas	Initiating process group	Planning process group	Executing process group	Monitoring & controlling process group	Closing process group
Project integration management	• Develop project charter	• Develop project management plan	• Direct and manage project execution	• Monitor and control project work • Perform integrated change control	• Close project or phase
Project scope management		• Collect requirements • Define scope • Create WBS		• Verify scope • Control scope	
Project time management		• Define activities • Sequence activities • Estimate activity resources • Estimate activity durations • Develop schedule		• Control schedule	
Project cost management		• Estimate costs • Determine budget		• Control costs	
Project quality management		• Plan quality	• Perform quality assurance	• Perform quality control	
Project human resource management		• Develop human resource plan	• Acquire project team • Develop project team • Manage project team		
Project communications management	• Identify stakeholders	• Plan communications	• Distribute information • Manage stakeholder expectations	• Report performance	
Project risk management		• Plan risk management • Identify risks • Perform qualitative risk analysis • Perform quantitative risk analysis • Plan risk responses		• Monitor and control risks	
Project procurement management		• Plan procurements	• Conduct procurements	• Administer procurements	• Close procurements

Table 2.1: Knowledge areas and processes

2.2.2 Stakeholders identification

Stakeholders, according to [1], are referred to as interested parties. According to [3], the process owner of the process in this case is Project communications management. The key information we need to think about while we identify stakeholders, is that it can be potentially anybody, who is concerned, impacted or influenced by our project. As first step, we identify all of the stakeholders. As a second step we can see evaluation of theirs possibilities to influence our project, and how much they are interested. According to the level of interest they have on our project, they will probably use their power to influence our product. I would also suggest focusing more on their likelihood to positively or negatively influence our project. In case we have stakeholders that are willing to cooperate, we could reduce the risk of project failure. On the other hand, if they don't like our project, we should focus more on explaining them, what is to be done, why and possible positive outcomes for them (not always possible). Anyway we should create strategies for important stakeholders to cooperate with them. This is an ongoing process. [1] also mentions that even stakeholders identification is an ongoing process which may be triggered again, when a new party starts to be interested in our project (by means of law change etc.).

Apart of these two main tasks [1] also talks about *strategy*, that is produced prior to *project charter* and is a high-level view on what is to be done. This project *strategy* is shared among all stakeholders.

2.3 Planning process group

These processes lead to determining the total scope, time and money needed to develop the whole project. While creating the whole budget, we have to think about possible risks that arise, plan product quality, communication among the team or for example procurement. That is why processes within this group are strongly connected and some of them have to be performed simultaneously. While project manager is trying to cooperate all these processes, he shouldn't forget to try to involve all possible stakeholders. They have usually deep understanding of the problem and area the project covers. They can also be very helpful while estimating time and budget for *activities*. The main core of the planning process group is a sequence of processes, that leads to breaking the whole project into small pieces – *activities*, that are easy to deal with. While considering these *activities* as small project, we can estimate their time consumption, scope and money needed. Going bottom-up back to the whole project, we can estimate the scope, time and money demand for the whole project. Let us have a look closely on the processes.

While [1] leaves a great deal on the choice of techniques used to produce necessary planning, [3] splits the whole process into smaller processes to define them more in detail. I here summarize some of the processes where applicable, to suit the way I learned to do them and find it useful so.

2.3.1 Requirements collection

According to [1], requirements are mostly distributed among *project charter* and project strategy. Since requirements are of great importance and they are usually used as base information for creating network graphs, [3] suggests to create a separate process, that will collect all requirements and suggests techniques to achieve best possible results. Among these techniques are questionnaires, surveys, interviews, or for example workshops.

2.3.2 Network graph creation

The process of graph creation consists of a few steps, which are to be performed step by step. Still there is often the need to go back one step and redo some of the work that already has been done. That is why I think that this should be just one process. The process owners for processes that are included in this process according to [3] are project scope management, project cost management and project time management.

- First thing we need to do, is to start breaking the whole project into smaller pieces – sub-projects. These projects can be later used as work packages if necessary. Then we keep on breaking these into finer pieces as long, as it takes to create *activities*, that are evidently easy to perform, measurable and understandable. This approach is called **Work breakdown structure (WBS)**. In [3] there is a separate process to do that and process owner is the project scope management. Since this process can be parallelized, but still has to be the first process, that has to be done [1] suggests that the responsibility owner is the project manager.

- Once we have done work breakdown structure, we serialize activities where necessary. That means if there is a *activity* that has to precede another *activity*, we have to serialize them. While different approaches result in different outcomes, we will not go into details about the method used. I personally found, that this creates a network graph by itself no matter how you visualize it, because all *activities* have to follow after the beginning of the project (or further) and precede the end of the project. This **network graph** is also widely used across project management support software.

- Then we go into detail on each of the *activities* and estimate costs, time consumption and resources needed to complete it.

- Once we have all this done, we usually input these information into project management support system, which will guide us through the integration process, completes the graph and uses algorithms like critical path, critical chain or resource leveling, to compute the best possible time schedule using available resources. It also gives us the answer on our questions about time, budget and resources.

You can see that if there is a change needed while applying the last point mentioned, we could be forced to use special methods, like activity splitting, to achieve better results. That is why you'll need to go back and revise one or more things you have done through the process. [3] uses the term *rolling wave planning* to indicate that planning is an iterative and ongoing process, not just one time shot.

[1] not only mentions the need to develop budget for the whole project, but also talks about the way project is funded. That could lead to a change in the stakeholder section, because there is a difference between a simple bank loan, that gives us just money and BOT (built-operate-transfer), where we will in the future operate the business (mostly applicable to large scale building projects as for example airport).

2.3.3 Plan quality

Quality is the degree to which were expectations of customers met. To plan quality we create standards and requirements that are measurable, or provable in other ways. These outputs are usually implemented as checklists, metrics or quality management plan. These

requirements are an integral part of cost planning, because if extra quality is needed, some activities will take longer than usual or demand more money. The process owner of quality planning is quality management. [3] suggest some specific ways to create desired output.

- *Cost of quality*, which balances the cost of preventing the project from failing some of quality requirements against the cost of actual failure.
- *Control charts* creates limits for each variable that is to be monitored and bounds that are not supposed to be exceeded. Then we monitor the actual performance of the project according to our preset limits. If a project slips away from suggested performance, we know that there is something wrong and we should put some actions into effect.
- *Design of experiments* is a process of creating pairs of experiments and desired outputs from these experiments. [1] also suggests for projects, which have a computer program as output, to create experiments with customers. That way we can identify early errors that can easily be corrected in future versions.

It is also vise to plan procedures such as quality assurance or quality control. They do not guarantee the complete satisfaction of customers, but they add to the probability of success.

2.3.4 Plan human resources and communication

Developing human resources plan should be done at least partially while creating network graph. That is because if we want to optimize the whole project time, we need the information about available human resources. Doing both at the same time we have more options to optimize, or adjust at least activities on the critical path. There are a few other possible outcomes of human resource planning.

- *Hierarchical charts*, that have breakdown structure and contains information about who is to whom reporting. They can also have the form of responsibility division charts.
- *Matrix-based charts* are mostly used for assigning responsibilities across the whole project. In this matrix we not only input direct responsibilities, but also the information about who is there to supervise, consult or just to be informed.
- *Staffing management plan* is a direct output telling when, how and under which condition the staffing requirements will be met. This is one of the most important parts on large-scale projects, because of the amount of work and number of employees that has to be achieved. This plan should be (if possible) consulted with appropriate HR department.

I personally found that in [3] is missing the act of planning communication among the team. The book understands as communication information exchange with stakeholders. It is true that people working within the project team are also stakeholders, but still it is not enough emphasized. Because communication channels are strongly connected to HR plans, I would suggest planning communication among the team as well while we plan HR. It consists of setting rules for meetings (information sharing among the team), reporting templates (down-up information sharing), and operative plan changes communication (up-down sharing). [1] also suggests doing regular communication feedback on both sides – stakeholder side and project team side.

2.3.5 Risk management

Risk is all about uncertainty. While we do risk management we try to reduce the uncertainty within the project. We try to predict all possible effects from all possible sources and their impact on our project. If we could predict all possible future actions, there would be no risk within the project and if the whole project planning was done properly, the project cannot end differently but successful.

My personal point of view on this is that people tend to think positively. How often do you ask yourself „what will I get for lunch?“, but how often do you ask „what if I don't get to eat for three consecutive days?“. The problem is whether we were taught by the society to think that way (mum telling you „Oh, come on! Don't be so negative!“), or we were born like this. I would suggest letting philosophers decide that problem. The point here is that we all trust in good results. That is why we need a systematic approach to ask questions, we might possibly dislike.

It should be said, that risk management handles systematically also opportunities that can help the project.

The stages of asking these questions according to [3] are:

- *Plan risk management*, where we decide about the form of questions we will ask about the project. We also decide about the way we will evaluate risk and possibly respond. We do that first, just to not be tempted to suit these borders and limits to the result in later stages.
- *Identify risk*, where we try to predict all bad and good things, which can happen during the project.
- *Perform qualitative risk analysis*, where we apply our risk management plan to evaluate the probability and impact each risk can exercise on our project. This way we split the whole bag of risks into categories that will be handled differently. We will for example try to avoid risk, that is very probable and will be a complete disaster for our project, but we will just accept a risk that is not likely to occur and has little to no effect at all.
- *Perform quantitative risk analysis*, where we try to express qualitative expressions by numerical values, so that we can measure them.
- *Plan risk responses*, where we make sure that all risks and opportunities are handled according to our risk management plan. We prepare plans to deal with risks that have great impact, or for example prepare plan to make sure an opportunity will come truth during our project. While creating these plans, we also have the opportunity to change the whole project plan to make sure some of threats will never come to affect our project.

Because this is the core of the work it is explained in detail in chapter 3.

2.4 Executing process group

The processes within this group lead to fulfilling the aim of the whole project. Here is where all the deliverables are to be created, services provided, or just programs written. These processes are usually the most time demanding considering the whole project. They

are also very normal to all manager functions, because they are the actual body of doing something. Here are the processes, which we are supposed to address with special care.

2.4.1 Team creation and information distribution

Though [3] doesn't not specify the order of processes following each other, we will keep the chronology going. First thing to be done while developing the project, is to create the team. On one side we have projects that might be part of a big company giving the project manager no control over the choice of employees available for the project. On the other hand we might have projects that depend on local people that need to be hired for the time being of the project. These problems should be already addressed within the HR plan.

A project manager is usually considered as the team leader of the whole project team. He should posses a great deal of soft skills that are necessary to negotiate, share information and influence others. There are a few areas that are considered as good to pay attention to:

- As the whole team is being put together, we should be familiar with the stages that each team goes trough. Some sources like [8] or [1] identify four stages of the team that are **forming, storming, norming and performing**. Some sources like [3] have five stages where the first four are identical and the fifth stage is **adjourning** which comes with the end of the project, when team has to move on to next project.

- There should be a system of appraisal for being a good team player in place. This system is supposed to motivate all employees to perform above expectation. It should give people the feeling that their work is valued by the leader.

- Project manager should be aware of the cultural differences that might arise during working in multicultural environment. These problems are usually solved by setting rules that are to be obeyed and are agreed upon during forming phase of the team. These are usually called *ground rules*.

- One thing that I found very useful while working with people in a team are so called *Balbin's team roles*. [11] identifies 9 roles in the team that are **Coordinator, Resource Investigator, Team Worker, Shaper, Company Worker/Implementer, Completer finisher, Plant, Monitor/Evaluator, Specialist**. It doesn't mean that we are supposed to have all these roles within each team, but it gives us rough idea about how will people react to specific tasks they will be assigned to.

2.4.2 Direct and manage project execution

As said the main core of the project is being done in this process. While [3] labels as the process owner the Project integration group, I would suggest to leave this responsibility upon project manager in small to medium scale projects. He is the one to know most of the information and his judgment is usually good. Nevertheless, he is the one who is in the end responsible for the whole project. In large scale projects I think it may be useful to take the pressure off project manager and delegate another person, so that project manager has more time to spend on controlling and changes that need to be done.

The core of the execution is to be performed according to the network graph that has been created earlier. While working on each of the *activities*, it is mandatory to give feedback on work progress in regular time intervals, to allow control mechanisms to be set

in place. The work should be carried out possibly most efficient, according to HR plan and corresponding to quality requirements. One thing we should ensure while fulfilling *activities* is that if something goes wrong, the report should be done as soon as possible to allow earliest possible work around. It should also be carried out taking in account applicable risks and possibly avoiding them.

Very important thing while performing the work is to keep an eye on costs of the activities. Usually there is a separate person responsible for procurement that has to follow local policies and law. For example some countries do expect business to keep bills for several years from all contracts for taxation purpose, but some countries are more benevolent.

2.4.3 Perform quality assurance, manage stakeholders

The process of checking quality is done earliest possible, when some of the areas described in quality plan are applicable. All tests and scenarios that were specified in quality plan are carried out. Quality checklists should be regularly applied and tested against the product. That way we can measure quality of the whole process leading to a quality output.

While quality is only measured by the stakeholders, we should strongly keep in touch while trying to identify possible flaws in the project. For example if we create a prototype of an IT system, we should go back to our customer to show and discuss the results. That way we can ensure the project will be regularly checked with the customer.

2.5 Monitor and Controlling process group

These processes run from the beginning of the work till the end. They get their information according to the communication plan. There might be a few different levels on which the information is gathered. For example there is just a simple graph showing progress of the activity for overall project overviews, but detailed hours spend for the purpose of team scheduling.

2.5.1 Cost and time control

While we try to control time and costs, we gather information about the progress of the work done. Two basic types of information are gathered:

- Actual cost of each *activity*
- Actual progress (earned value) of each *activity*

Both of these information are usually gathered by project management support system. That way it is easy to follow the progress of the whole project, where a lot of different activities are present. Support system adds all values together and calculates actual cost of the whole project (AC) and project earned value (EV). These information are usually used to provide different analysis. [3] suggests a few analysis that we will have a closer look at:

- *Performance review*, which takes in account buffers that were inserted in the project „just in case“. By counting the amount of buffers that are still available to those, which are already taken, we could estimate, if the project is still on track. It shows areas (where most of buffers are already used), that might need corrective actions to be performed.

- *Variance analysis* tries to show the current variance of the project with the tendency of it in time horizon. There are a few basic indexes that are used:
  - *Schedule variance index (SVI)* that shows current status of the project against the planed status. The formula of this index is $SVI = EV - PV$, where PV is the planned value that we were to achieve till today.
  - *Cost variance index (CVI)* that is similar to SVI, but shows the same thing for budged. The formula is $CVI = EV - AC$.
  - *Schedule performance index (SPI)* that shows the actual rate with which the goals are met. That is, if we are working faster or slower than we planned. The formula is $SPI = EV/PV$. If $SPI > 1$ then we are actually working faster than we planned.
  - *Cost performance index (CPI)* shows if the current cost is according to the plan. The formula is $CPI = EV/AC$ and if this index is lower than one ($CPI < 1$) then we are using too much money for what is being achieved.

  Combination of these indexes can show us how we are doing overall on our project. For example with parameters: $SPI = 1.2, CPI = 0.93$ we can say that the work is progressing much faster than we planned, but for additional costs.

- *Forecasting* future development of the project is very useful, because it can give us not only the idea about how we perform now, but how will it impact the whole project. That is how much increase are we to expect at the end. Two of the commonly used indexes are:
  - *Estimation at completion*, where we take the current status of the project and its trend, and project it to the whole project. That way we estimate how the budget and time frame for the whole project changes.
  - *To-complete performance index* shows how much we have to improve our work from now on to meet the budget and time frame that was planned.

These analysis are used to get some insight into the project. They are also helpful to decide, whether it is already appropriate to apply remedial actions, or put some changes into place. Depending on the severity of the problem we are faced with, it might be also necessary to consult the progress with customer, or in the worst case to stop the whole project.

2.5.2 Quality and risk control

After each activity is done, or for example periodically during the whole project, it might be useful to check quality of the outcomes. We gather the results of the quality assurance and, if necessary, we try to find reasons, why the tests failed. Usually 20% of reasons are responsible for 80% of quality decrease over the whole lifetime of the project. Having identified the reasons for quality decrease, we can suggest remedial actions or work-arounds to resolve the problem.

Here is where also the risk control comes in place. Here is where we observe, if triggers that are described in risk management plan are being pulled. If we identify a risk, that needs a risk response according to the risk management plan, we ensure it will be applied. The same approach is applied, if there is a fall-back plan needed. Apart of this we try to re-asses risks, identify new ones and remove from the risk register risks that are no longer

applicable to our project. We could also request changes to avoid some risks that are now more probable or their impact increased.

2.5.3 Integrated change control

What most of the projects I have been working on was suffering with, is the amount of changes that were requested. Requests come from various sources. It is usually the customer that wants to add some extra functionality to the project for the prize of the old system. Then he wants to add just a little bit more. This is called *scope creep*.

We should adopt systematic approach that makes sure that each change request is documented. While there is a specification for what is to be changed, we can estimate the impact of the change on the whole project. We might be forced to increase the budget of the whole project, if we encounter a major change. If there is already a documented version of the change, there must be somebody responsible for approving or rejecting the change. Usually this responsibility is distributed among the whole team. For example small changes, that have little to no effect at all, are approved by the team manager, who is responsible for that part. But major changes, that need revision of the whole budget, need to be approved by the customer, because it takes usually more resources and money to implement the change. So each change that has been approved, has to be documented and appropriate changes to project plan are to be applied.

2.6 Closing process group

This process formally closes the whole project. It has to make sure that all formal parts of the contract are fulfilled and stakeholder expectations were met. It does the actual handing over of the whole deliverables including its documentation. In case the project has been terminated other way than with success, we should document the reasons for project shutdown.

Where applicable, project manager should document lessons learned from the project for future reference.

Chapter 3

Risk management

In chapter 2.3.5 we discussed the origin of risk management from the psychological point of view. [7] discusses the same thing from a historical point of view showing, that the way to systematic risk management wasn't an easy one. The need to develop projects that are risk-safe prevailed by yielding better results. It also discusses in detail the basic concept of dividing risks into external and internal. This division of risks depends on the point of view, because a risk that a project manager labels as external can be an internal risk for his boss, because it can still be handled inside of the company.

Let us now have a look closely at the way it is done. We will keep on following [3] to adhere to current norms.

3.1 Plan risk management

The process of planning has two stages. The first one is a manager stage, where the manager has to decide about the risk team, risk team meetings, risk management budget and similar things that are necessary to ensure smooth run of the whole process. The second stage is strictly risk oriented. Firstly the team should decide about the methodology that will be used through the project. Because each methodology of risk management has a bit different inputs, we shall just say that all the initial values are set. It usually consists of:

- *Risk categories*, which have a breakdown structure, where we categorize risk according to its source.
- *Risk probability and impact*, where we explicitly set the values for something being very probable, so that there is no discussion about the actual value of the risk. The same thing is done for time, cost, scope and quality.
- *Stakeholder decision*, that states to which degree is risk acceptable. It is the actual value of risk tolerance for each stakeholder. This decision should be very well documented.
- *Reporting format* of all documents and information that will be gathered through the risk management.

Once we have all these decisions, we apply them and continue with the actual risk identification.

3.2 Identify risk

Identifying the risks is an ongoing process, because new risks may arise during the project. All stakeholders are also encouraged to identify possible risks. They have often thorough knowledge about the area that we work on. Most of the work is done usually by the risk team. The way the risk is identified is usually informal and based on previous experience, expert judgment or risk checklists from similar projects. Some of the ways I have seen it done are:

- *Brainstorming* which is the most common way. The team comes together and they freely think about possible risks for the project. Because each person thinks a bit differently, we gather usually a great deal from all the risks. This is usually also the first method that is used.
- *Checklist analysis* takes in account previous experience with similar projects. It is not necessary to have an application specific checklist, but it is definitely helpful. Going through the checklist we identify risks that we omitted during brainstorm. It is necessary to say that some of these checklists can be downloaded from Internet and that there are specialized companies selling these checklists.
- *Expert judgment*, where we ask a specialist in the area. It might be a project manager that led similar project before, or using Delphi technique among several of these experts.

The output of identifying risks is a so called *risk register*, which contains list of the risks that were identified. It has also space for additional information that will be added in future. Sources differ in what additional information is necessary.

3.3 Perform qualitative risk analysis

Qualitative analysis splits the whole risk register into smaller areas according to different criteria. This is done to ensure that the most important risks will not get forgotten or omitted due to large number of risks. For example if we have one 90% risk in one area and the rest of the area has close to no risk at all, the whole area will not be seen much risky. That way we ensure that this important information about the severity of the risk will get propagated through the whole risk management. Some of the criteria [3] suggests are:

- *Probability and impact* are the first big areas. According to our risk plan, we think about the risk and put it in the category of how probable the risk is. Then we place it in the impact category it belongs to. Both are done verbally and without any numbers. Then we know that if a risk is very probable and the impact is big, then this risk is very important for us. All this information gets recorded and will be evaluated in the quantitative risk analysis.
- *Risk categorization*, which splits the risk register according to the origin of the risk, or according to the area it has impact on. This shows, which areas are riskiest and which are safe. We naturally concentrate on the areas that are riskier.
- *Expert judgment* is almost always a good way to get support, or ask if there is anything we omitted. An independent view also tells us, if we are on the right track.

Collected information is recorded in the risk register to the corresponding risks. It also gives us relative ranking for each risk that tells us, which risks are the biggest.

3.4 Perform quantitative risk analysis

There are several different approaches that treat the quantitative analysis. We will start with the one that is the most different to all of them.

3.4.1 Range quantitative analysis

To each activity we gather different opinions on the cost and duration of the activity. We can use interviewing to gather these opinions, or for example Delphi technique (although we are not trying to reach a consensus, but only to gather the opinions). If we get values that are very similar to each other, there is little or no risk at all that the activity will fail. If the range is big, then there is a certain degree of risk (we are now not trying to name it). Once we start adding up all these ranges, we might be able to count the range for the whole project. Using a distribution function we can estimate the degree of uncertainty we have in the project (the lower bound has a probability of 0% while the upper bound is 100% of success). As can be easily seen this approach does not identify all risks, but only talks about money and time. Hence it is easy to see that there might be a better case than lower bound predicted (which is not a bad result), but there might be also a worse case then the upper bound.

3.4.2 Risk quantifying

There are a few commonly used ways to achieve a numeric value from a qualitative expression.

- *Expected monetary value* is an analysis that is pretty straightforward. According to our risk plan we simply translate qualitative expressions (for example „very probable“) into its numerical values (probability 0.65). Once we have done both probability and impact we multiply those values. Because this approach is usually used to compare different scenarios, a decision diagram [14] is used to do that.
- *Modeling and simulation* uses a model of the project and uses a random number generator to repeatedly evaluate all possible scenarios. Typical method for it is Monte Carlo simulation.
- *Expert judgment* is always a good way to double check your results.

The monetary value of the risk is usually also stored within the risk register.

3.5 Plan risk responses

Once we have our risks identified and evaluated, we need to decide, what to do with them. The approach follows the risk plan, where is statement of risk tolerance. That is the degree of risk that we can accept without risking „too much“. This level should be consulted with all stakeholders so no surprises will arise. So the ways we can handle risks are:

- *Accept* the risk. This is the simplest way, where we do not prepare any fall-back plans or anything else. If it happens, it will exercise its impact in full measures and we will have to do work-arounds. This approach shouldn't be adopted for anything that may result in failing the goal.

- *Mitigate* the risk to get it into acceptable bounds. That is we decrease the severity of the risk (not just by rewriting the numbers, but actual action will be taken). For example we might build our factory in other country that has more stable government. It usually cost some money to take the action. This might include a fall-back plan that will be set in place, if this risk occurs.

- *Avoid* the risk is the best solution. We change the project so that the risk will be no longer applicable to our project. This is not always possible and can generate additional risks. Risk team is advised to use this wisely with the knowledge that the whole risk management process needs to be revised.

- *Transfer* the risk to a third party. We do that if there is a risk, that we cannot avoid nor mitigate, but we know it has major impact on the project. We can make the customer sign for this risk (he will pay for it), or use a third party such as insurance company.

Similar division can be done for opportunities. Since it is normal for us to naturally exploit opportunities, or even worse count on them, we will not go into further detail.

Having all these information we can set triggers through the whole project that will tell us, when a risk was encountered. The risk plan should be communicated to all stakeholders, so they are aware of all the risks and work pro-actively to avoid them.

Chapter 4

Requirements specification

The system should implement all parts in risk management process. Though there is a specific way I would like to do it. The core of the work is to help planning and identifying the risks. Since this is mostly not an algorithmic process, I suggest a program that will be helpful by identifying risks that the authors forgot. The system of helping is specified bellow. As this system is trying to help improve the value of the whole process, it will adhere to the 27000 ISO/IEC normative family ([5], [4], [6]). Using the program will (optional choice) assure, that if used for information technology branch, the product will adhere to these norms.

Since the program is complex we will go through each stage of the risk management and specify the system step by step.

4.1 Plan risk management

The planning of risk management will consist for us from two part. The first part is to create a *common vocabulary* that will do the translation between what is stored in the database as previous experience and our current language. This not only allows variation in how you call things, but will also allow using of a different language to do the whole process. The second part is to set bounds for all possible variables within the system. Here is a list of variables that the user can adjust within the system.

- Time-is-money ratio (if we work longer, it will cost money from the contract)
- Levels for risks that can be avoided, transferred, mitigated or accepted
- Type of formula to aggregate risk probabilities

These values will have at the beginning a based-on-experience value, that should be consulted between the user and his supervisor and in the case of need, changed into different values. These bounds will not influence the actual values of experience in the database, but will influence the way they are interpreted.

4.2 Identify risk

This is where the core of the work is. The point of the work is to help the user to not forget the risks that he might have omitted. The idea of how it works is that we will use previous experience to create areas, where risk is located. As they say a picture is more

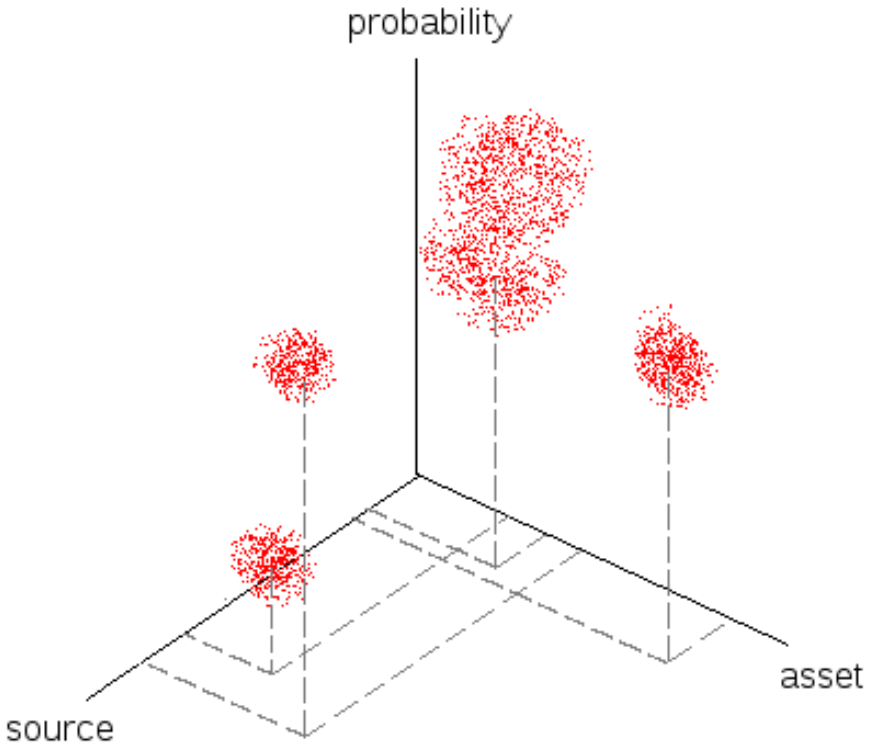


Figure 4.1: Proposed visualization of risks

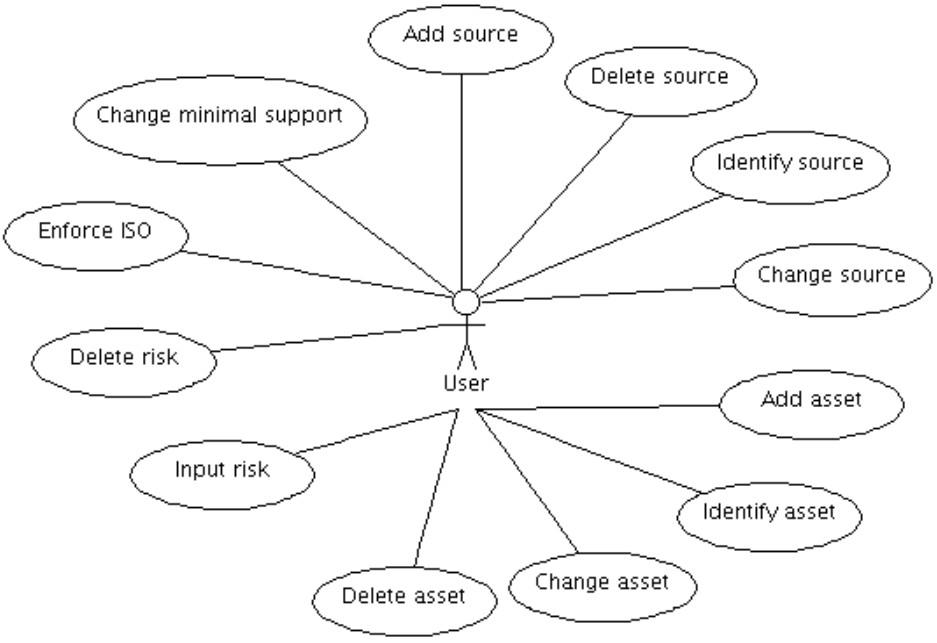


Figure 4.2: Use case of risk identification

than a hundred words: On the picture 4.1 you can see that we will split the risks according to the source of the risk, the asset it will influence and the probability of the risk. That way we create a 3-D cube that contains all our risks. The axes of the graph are very important here, because we will use data mining procedures to handle the cube.

On the picture 4.2 we can see what is expected from the program during this phase.

- The program has to be able to let the user create new risks and delete those that are not needed anymore.
- With risks he should be able to identify its source and asset it will have influence on.
- The program should extract information from database and supply them to the user. This information has to be in form of risk sources and assets that the user might have omitted.
- The program will use data mining processes to find risk sources and assets.

4.3 Perform qualitative and quantitative risk analysis

We will perform both risk analysis at the same time. That is because from my point of view, qualitative analysis is pretty much always some kind of quantitative risk analysis.

On the picture 4.4 we can see that the user has not many possibilities to influence the flow of the analysis during this stage.

- The program should use questionnaire evaluation to asses quantitative risk analysis.

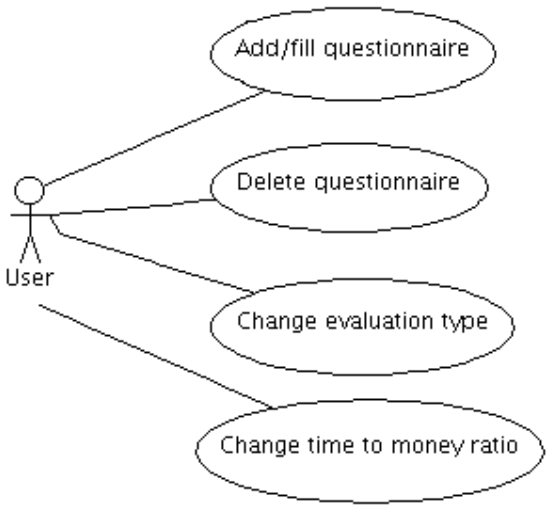


Figure 4.3: Use case of risk analysis

- The program has to allow the user to print out a questionnaire.
- Minimum of three different ways to asses the questionnaires is expected.
- There must be a way for the user to fulfill multiple questionnaires by hand and delete those that are no longer needed.
- The program should extract values of risks from the database and supply them for the user to compare with his values.

4.4 Plan risk responses

This is the phase when it all comes together. According to the risk management plan, the program will ask the user to plan risk responses. The possible responses are:

- *Accepting* the risk will simply delete the point from view, because the risk is not enough important.
- *Mitigating* the risk will lower both time and money needed to cope with the risk. It will also ask for the prize of mitigating to compute the complete budget. It checks, if the risk is already low enough to accept the change.
- *Avoiding* a risk will delete the point. It is advised to do that wisely, because new risks may arise.
- *Transferring* the risk will also delete the point and asks for budget arise. Each transfer costs something. You can transfer it to the customer, but he will surely give you less money for the whole project. If you ask a third party to do that, you will have to pay insurance.

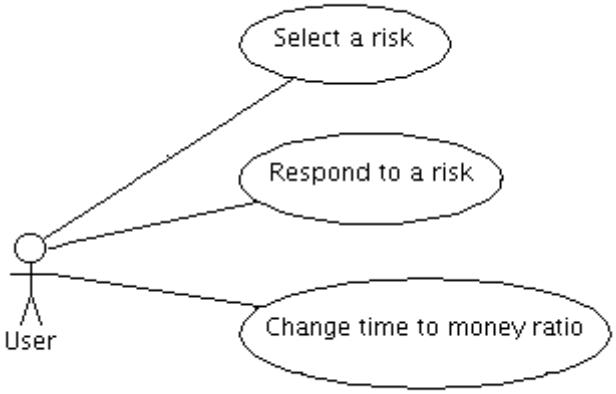


Figure 4.4: Use case of risk Response

The program will check for each risk, if the approach chosen by the risk team is appropriate according to the risk management plan. It will also create the complete estimated budget for the risk management.

On the picture 4.4 you can see that the thing that needs to be solved is only an efficient way of selecting risk, because response is only user's responsibility. Program will only check, if risk is low enough to be accepted. So the program is expected to:

- Select among responses and make possible to add all information needed.
- Respond to a risk, or multiple risks at the same time.
- Preferably the program should provide a checklist of responses for the user to follow.
- The program should in the end provide summary of risk assessment. Some of the things the program should evaluate are:
  - Amount of risks, risk assets and sources.
  - Summary of project risk before risk responses were put in place.
  - Summary of project risk after the risk management is completed.
  - Compliance to ISO norms.

Chapter 5

System design

The structure of the program is singleton-based. Singleton [2] is used as perfect data storage for multiple data access. That means we access the same data from more points of view. It also provides user-sided buffer, so not all operations have to be performed directly on the database side. Each phase of the project accesses the singleton with different demands, which creates single point to access all the data (Data Access Object), making it very easy to manage changes done during analysis. This object is also the complete stateoftheart of the project, so if the demand for saving the project comes, it is only necessary to persist this object. The data should be stored in a professional database to ensure consistency, multiple access and allow later multi-user environment.

5.1 Identify risk

The risk identification is for us the most important part. We will try to make this identification as pleasant as possible.

5.1.1 Suggested process

The way user is expected to work with the program follows.

- We will let the user do his usual risk identification. That means usually brainstorming, which results into risk register. Why do we let him do this job, if we could help it? Yes, we could help it, but even if our program has the best possible knowledge so far, each project is unique. That is why a new project can contain risks the program does not know yet.
- Input the risk register into the program. Translation into common vocabulary is necessary. This translation will be done by a language recognizer. This recognizer will understand English language and thus gives us precise information about which words correspond to sources and assets.
- Analyze the risk register to find all assets and risk sources in the current project. The program will check, if the user didn't forget some assets or risk sources. That will be done on the basis of previous experience. In the database we can check, that if the user inputs as an asset „Internet server“, there is a big chance that there should be a risk source „hacker“ (lots of risks in that area). For finding these assets and sources, the FP-tree method will be used as it is considered one of the best. The program also

checks for ISO/EIC compliance in the form of not omit-able assets, because the norm describes assets and risk sources that need to be taken into account.

When following the process we should have all possible risks identified. What we need to do, is to have a closer look at some of the details.

5.1.2 Data cube

- The *source* axis contains all the sources possible. They are not only listed, but there is a hierarchy build for all the risks. The top of the hierarchy is „source“, the second layer can be for example „external, internal“ and the leaf nodes are names of the risks.
- Similar hierarchy is done for *assets*.
- The *probability* axis has different division which has finest division into real numbers (percentage probability). The middle division (more coarse) is into *common vocabulary*. The top of the hierarchy is the complete probability that something will go wrong.

The values within the cube are of two dimensions: time and money. It can be easily seen that each risk, that we will have in the risk register, can be inserted into the cube, because the information we need is only: risk source, asset affected, probability, time impact and money impact. One thing that we need to mention is that the cube is in fact 5-D. The two dimensions that are not shown are time and money. The problem of showing 5-D graph is obvious, so the suggested solution for visualization of them is to color each risk. The risk is by default white. The time axis will have red color for each point and money axis will be blue. That means the more severe the damage is the more red or blue will get. How do we combine them? Yes! The points will get purple.

5.2 Perform qualitative and quantitative risk analysis

We will perform both risk analysis at the same time. That is because from my point of view, qualitative analysis is pretty much always some kind of quantitative risk analysis.

The suggested way of performing this analysis has three levels.

- Let the risk team asses each risk. This information gets recorded.
- Generate questionnaires that will be used among experts to assess each risk. This information gets also recorded.
- Compare these numbers with experience taken from database.

All these information gets recorded in the background of the cube. There is a new cube created for this current project that will contain only risks that are appropriate for our project. By selecting the information from database relevant to information stored in the cube for current project, we might extract values the user can compare to his results.

5.3 Plan risk responses

Planning response is only simple filling the database with the values supplied. Thus we fill the whole risk register and we have complete information for next projects.

Chapter 6

Implementation

According to system design in chapter 5, the system was implemented. There were various corrections to the design made. Some of the features the system was proposed to have, turned out to be more or less useless or in the worst case rendered the work with the tool impossible. Decisions done within the process and the whole implementation including the reasons why changes were made, are detailed below.

6.1 Environment selection

The task is to program a prototype graphical tool to provide risk management support. There are requirements that need to be fulfilled. Among these requirements are.

- Graphical front end for the user.
- OpenGL support for cube visualization.
- Preferably language recognizer for that platform that is ready for use.

These requirements are very hard to combine, but java language showed that it can combine all 3 of them. It has swing, which is easily used for graphical applications. The Netbeans platform for java has OpenGL support, both heavy and light weighted. There is a language recognizer written in java called MorphAdorner. The combination of these three aspects makes the choice simple. We will use the java NetBeans IDE to create our experimental tool.

6.2 Data storage

As data storage was chosen Oracle platform. The machine it is by default connecting to is **Oracle Database 11g Enterprise Edition Release 11.1.0.6.0 64bit Production**. This platform was chosen, because it is considered one of the best among database servers, and because its usage is pretty simple. There are multiple tables within the database created. If they don't exist, the program will auto-generate these tables with empty content.

Currently there is a bug within the implementation of the driver that is out of control of the programmer, which is that Java persistence API (application programming interface) with current Oracle driver is not able to figure out which tables are already present, so it always tries to create all tables. This operation fails most of the time showing error output

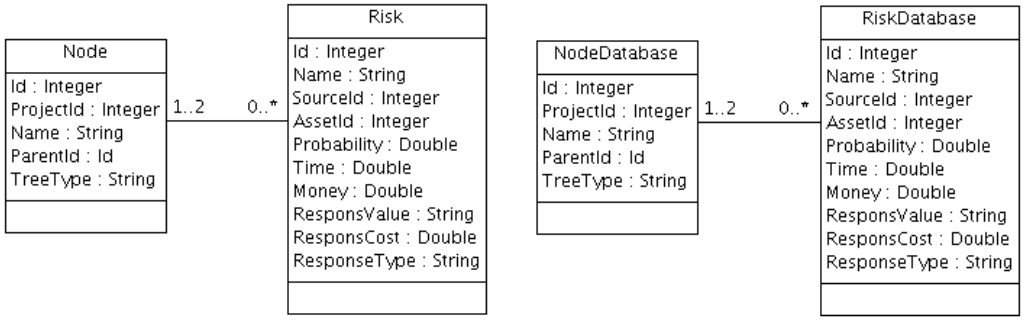


Figure 6.1: ER diagram

to the log. Having this operation fail doesn't hinder any use of the program, and will be probably fixed by the next Oracle database drivers.

As can be seen on the picture 6.1, there are two very similar tables to be created. They are divided into two categories:

- **Current project data tables** that hold the current project data, such as assets and sources identified during the analysis, risk responses to each of the risks etc.
- **Past project data tables** that hold a complete history of all projects done with the tool. This is the base of knowledge that is used for data mining. It contains not only risks with their response and costs, but it also has the sources and assets that were used in the project. It should be said that it is highly possible that the structure holds more assets with the same name, but different id, bound to different risks. The problem is that asset name is not necessarily unique thing.

We chose to create to separate, but almost identical tables for multiple reasons. One reason is to make a clean division between the risks that are used in the current project and those that are used for data mining. We should think of this scenario this way, that we are creating backup of all projects that were created. Having these backups stored creates history of all projects, and can be thus considered a data market for data mining. The other reason was to try out inheritance within Java persistence API (JPA). It was a big disappointment that JPA doesn't allow any inheritance among tables. Objects, that can be stored within database, need to be plain old Java objects (POJO).

These tables are filled with data supplied by the user. There is though one exception to this rule, and that is not-omitable risks. These risks come from the ISO 27000 family. There is a normative part in the norm ISO ([5]) that was translated directly into knowledge of the program. There were assets identified, that cannot be omitted, and thus make sure the project is ISO compliant. This information is not stored within the database, but is a part of the program by itself.

6.2.1 Data representation

As stated before the program is build around a data singleton that holds all information, making it easy to access data from different points of view and getting always up to date data. There are in fact 3 types of data that are stored.

- **Risk sources and assets**. These are stored in a structure of a tree. This tree can be directly visualized for the user to handle it (adding new nodes, deleting, moving). In fact there are 3 trees that are held. First two are holding the current project assets and sources. The third tree holds database information, where sources and assets are merged to one single tree (to reduce the amount of tables). This tree is used for phrase identification.

- **Questionnaires**, that were done within the current project. There are different approaches to evaluate these questionnaires and the user is able to add, delete and remove these. They are not stored within the database, because no further use for them was found.

- **Risk register** is the basic structure in risk management. Since multiple studies were done on the amount of information that is supposed to be stored within the risk register, we should note that only a few were common (name, money, time, and probability). The other fields very strongly depend on the specific field they are trying to handle. What our risk register contains is:

  - **Name** of the risk. That is the complete sentence given by the user.
  - **Source and assets** that were identified for the risk.
  - **Probability, money and time** that the risk contains. This information comes from questionnaires evaluation.
  - **Risk response type, actual response, and its cost** are values given by the user by assessing the risk response.

6.3 Identify risk

The risk identification has some stages it has to go through. As stated before we let the user to do his usual risk identification. What we expect him to have afterwards, is a list of risks in normal sentences. These sentences are very close to scenarios, but still are enough general to aggregate multiple scenarios. Typical example is: „A hacker can attack our web server“. These sentences are split to words. There is actually a whole process behind splitting, which includes language classification and finding the base form of the word. Once this splitting is done and we have all the base forms of words, we try to recognize phrases according to knowledge in the database. That should add to each sentence asset it influences and risk source. Phrases that were recognized are marked so that the user clearly sees them. Different colors for assets and sources are used so that user has control over how many words are recognized (see 6.2). User can freely adjust the recognized words among synonyms, if there are any. He can also add, remove and change assets or sources already present at will. His duty is to ensure there is exactly one source and one asset at each line that represents a risk. Once he is happy with the sources and assets recognized, these sentences are translated into risk register. Risks, that have wrong number of assets and/or risks, are not translated and marked so that the user can pay more attention to them. Further are used only risks that were properly identified.

User has „whispering“ for him ready. He sees in a window all the assets and sources that were found as being related to those, that are already identified. The ISO norm based risk assets are used for „whispering“ as well. It is up to the user to determine, whether to use them or not.

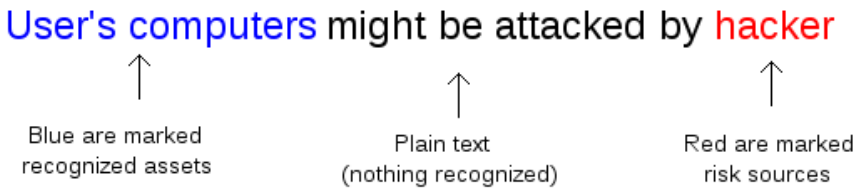


Figure 6.2: Example of phrase recognition

Here comes one big question about this approach. Once a word has been recognized, it cannot be „unrecognized“. The only way to make it not recognizable for the tool, is to actually use a different word (synonym) for it. I was considering this as a bug or a downturn of this approach. A specific way of handling this was set in place, to make it possible to mark a word as unrecognizable. Experiments showed that this approach makes the work much easier. The problem comes later, when analysis is done, because it has shown that using this approach generates a lot of synonyms for the same meaning. This problem is language related and is elaborated in following chapters. Feature, making some parts of the text unrecognizable, has been therefore turned off to make the user think more about what he is marking as asset and source.

6.3.1 Phrase recognizer

The first phase in the process of detecting risks is language analysis. This analysis has been discussed with people from Speech@FIT. This is also a small thank you to them for setting me on the right track.

First approach chosen is called **stemming**. This approach works with single words, trying to find its stem. The problem it runs into, is using words like „better“ which has its true form of stem „good“. Stemmer is very easy to implement, but it was found that its language capacities are not sufficient for our use.

Deeper approach is called **lemmatisation**. During this approach we work with whole sentences, trying to recognize theirs lexical category and therefore find appropriate lemma. Lemma is the canonical form of the word (it might be different to its stem). The process of finding lemmas is difficult for English, because of its large vocabulary and the amount of irregularities. Because it wasn't the aim of the work to create such a tool, an open-source solution was used instead. The program is called Morph Adorner [10]. It has been integrated into the project so that its use is transparent. Unfortunately using MorphAdorner makes the application work sometimes very slow. The loading time of application is therefore around 8 seconds, and each language recognizing is visible as a delay of the tool. To make it easy to understand this approach, see picture 6.3.

The use of this approach is pretty straightforward. We let Morph Adorner create lemmas of all words within the text user supplies the program with. Once we have all its lemmas, we try to match these lemmas to assets and sources of risks we already know. The process has some priorities that were hard-coded into the program. First place it looks for matches are the trees of already identified risk sources and assets. That is because once we identify a risk source or asset, it is very probable, that we will use it again within the same project. If none of them is matched, next in line is upon unforgivable assets (according to [5]). If

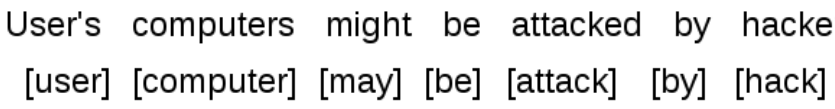


Figure 6.3: Simple example of lemma creation

both of these fail, we look in the database of projects that were already created with the tool. That makes it easy to reuse all the knowledge that is known to the program. It also makes the user use the same assets over and over again, which is the basic assumption for the whole process to work. After all these matches fail, we let the word be as unknown, or simply not label it anyhow (leave it as plain text).

Since Morph Adorner is a complete solution, let us just have a look at some of the more interesting aspects of this part that were found. First big problem is language barrier. It is not that one wouldn't understand English, it is the way English is built. Having a lemma of some words isn't the only base a word can have. Simple example is „to hack". It is a verb that can regularly be used. If we ask Morph Adorner to give us a lemma of the word „hacker", it gives us the lemma we expect which is „hack". But if we ask for lemma of the word „hackers", the lemma will be surprisingly „hacker". The reason behind this behavior is that Morph Adorner uses so called one level English. That means for each basic word (a lemma) is one way to change it to a different word. So from a verb „hack" we create „hacker". We created a noun out of verb. There are various ways of creating other noun from a noun (for example by creating plural). Morph Adorner finds the last change that has been made to it and provides us with result of undoing such a change as a lemma. So if we would like to get to the shortest possible lemma, we would need to call Morph Adorner multiple times. The problem with such an approach is that Morph Adorner is a lemmatizer, which needs to have some information about the sentence we work with (context). Undoing the first change can change its lexical category and may render the sentence senseless.

Second big problem identified during the use of a phrase recognizer is the ambiguity of English language. Here is a simple example of such a sentence: „Bill sold the invisible man's hat". Now tell me, is there an invisible man and his hat was sold, or did we sell invisible hat that belongs to him? This example shows that it is hard to decode the information within the sentence. It is even worse because with some words you cannot be sure whether it is a noun or verb. Is „start" a place where you stand just before the competition, or the thing you do after you hear starting shot? This problem runs deep inside of the proposed project. Consider having „hacker" as a source of a risk. This is pretty common among normal IT projects. Each verb „hack" will be labeled as risk source although it doesn't make sense. The proposed solution to this problem is to check for match between lexical categories. This approach made most of the expected matches not found, so it has been removed. For the user we suggest to reformulate the sentence in case he runs into these troubles.

6.3.2 Not-ommitable risks

According to 5 the program should support normative family ISO 27000. These norms ([5], [4] and [6]) talk about various aspect of project management in the area of information

technologies. They handle mostly the area of information security. Since some of these forms only point out the code of conduct for a project manager handling the area, the norm [5] contains in appendix A normative part. This part is one of the most interesting, because it can actually be proven that the project adheres to the norm according to this normative part. Since this part has already a tree-like structure, the transition between this norm and our program is pretty straightforward. In each of the control objectives and controls, all possible assets are identified. Unfortunately the norm doesn't specify any risk sources, but still this asset input is very valuable. So this normative appendix is directly translated into knowledge of the program. Since we are internally using a tree structure to keep all assets and sources, translating a tree-like structure from the norm is very intuitive. A complete list of assets identified from the norm is in appendix A.

User has the option while identifying risks to turn on „whispering" of not-ommitable risks. That means all assets that are mentioned within the [5] norm have to be present in the project. It should be said, that this normative help is not enforced during the whole process, because that could render the process impossible in the event of having some of the assets not applicable. There is a few ways to handle this problem in case we would like to enforce the actual norm more strongly. One of the ways is to give the user ability to change not-ommitable risks. That means deleting some of them that are not applicable. This approach has big advantage, if we would like to make these changes permanent, because we will hardly ever change our business so dramatically that we would need to change the structure back to original. The reason why there is no such a chance, is that once we allow the user to freely change anything that comes directly from norm, we actually loose the possibility to independently say that this norm was actually fulfilled. The worst possible outcome can be that the user deletes all not-ommitable risks, after which the program will consider every project done ISO compliant. The second (preferred) way of handling the need of enforcing is to simply transfer not-ommitable risks into our local asset tree, without actually attaching any risks to them. This approach has been made possible to handle the event of having an asset that is not applicable.

The preferred use of not-ommitable assets is to give the user some basic idea about how to structure assets and sources. Because if he starts working with it, it will eventually become his natural to work according to these guidelines. Therefore his normal way of performing risk analysis will later be ISO compliant. The importance of this basic structure goes even further, because if many ISO compliant projects were made, this structure will eventually cross over into the database of projects as one of the most common patterns and therefore will produce „whispering" results very close the ISO family. So shortly we could say that this ISO structure (in case of its usage) is expected to be found even in the database as one of the most common pattern.

6.3.3 Data mining

The data stored within database is later used in a few different ways. First of these applications is to „whisper" assets and sources that the user probably omitted. Let us now have a closer look at the way these parts of risks are identified.

First pretty natural way of mining data from database, is the usual way of data mining. That means we try to identify frequented patterns within the database of projects. To support this feature, project assets and sources are stored within the database including the information about project number. This numbering is done internally, without the user even noticing it. To find frequented patterns we consider each project as a single database

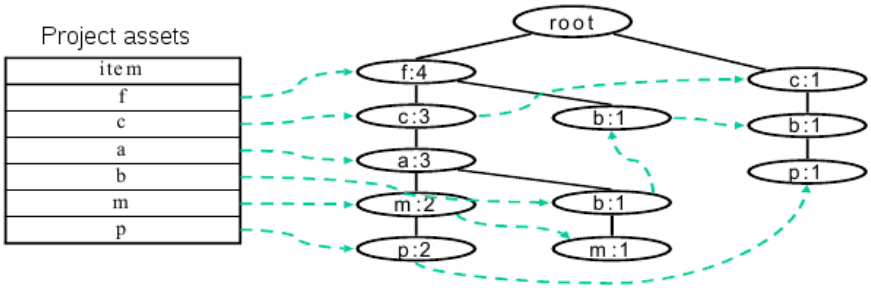


Figure 6.4: Building structure of FP-tree [9]

entry. Items we search for are mixed risk assets and sources. That means we see project as a set of risk assets and sources, included within the project. Since there is no need to try different approaches to data mining, the best of practice method was used. The method implemented uses FP-trees to find all frequented patterns without the need to generate candidates. That makes this approach very powerful and fast.

The FP-tree algorithm works in two phases. In the first phase the FP-tree is build. We go once through the whole database and compute the occurrences of each risk asset and source. This is necessary for the building of the FP-tree, so that it will be the most efficient. Once we have these occurrences we sort all sources and assets from the most common to those that occur only once. Having that done, we need to go through the database again and build the actual tree. In each project we identify the most common item and check if the root does contain it directly. If yes, we increase the value of that node and move on to the second most common item. We follow this till there are no items in the project left. Then we move on to next project.

As we see on the picture 6.4, we build the FP-tree according to the occurrences found in the first run. This way we are able to represent all information needed for frequented patterns generation. This is where the normal data mining process ends and my own modification starts.

Once we have FP-tree and we understand, that a frequented pattern is a path along a tree branch to a certain node, we can simply change the procedure of generating frequented patterns into check for them. We go through the current project and test each risk source and asset against this FP-tree to see whether there is a frequented pattern that does include it. Here was another decision made, that we will be preferably conservative about risk suggesting, so that we don't overwhelm the user with parts of risks. Usually if we would like to find all frequented patterns that contain the node, we must go through the tree, search for this specific node, and check if its occurrence is frequented enough. If yes, we would need to go to children nodes of the node we just found and test all its offspring, if they are part of this frequented pattern. In the worst case, if you hit one of the first nodes after root (in 6.4 could be the node „f"), you might end with all its offspring as parts of frequented patterns (depends on the level of support). So we only use the node's parents to whisper them to the user.

In the work we found it very useful to go one step ahead and try a different approach. We will do basically the same data mining approach, but we will change the data we work with. As one single database entry we will consider each risk. The effect of this approach is that we are trying to identify the most common 2-tuples among all risks. It is to be said,

that some risks (although they are different) have the same asset and source. For example „User wants to add examples to documentation.“ has the same asset (documentation) and source (user) as risk „Documentation is too complicated for the user“. So some of these risks are preferred to others, and that is exactly what we are trying to achieve while mining. Tests showed that this approach is not vulnerable to the problem described above about having too many descendants in the FP-tree. In the beginning, only one method was used for both approaches, but there were almost no assets or sources identified with the second approach. A deeper analysis showed that the FP-tree build with this second approach has always height of 2, which defies the problem with too many descendants and a separate algorithm was used for this type of mining. This algorithm already checks for frequented patterns both ways up and down.

There are two main attributes to data mining. They are called **support** and **confidence**. Let us have a closer look at each of them.

- **Support** is a value that shows how often is this frequented pattern found. This can be either absolute value, which is very rarely used, because of its obvious drawback of getting old very quickly with addping items. The more commonly used value is a percentage that marks in how many database entries it is found. 1% means that one in a hundred entries does contain selected frequented pattern. This value has no other meaning, but to select the most common frequented patterns. If we set support to value $1/N$, where N is the amount of database entries, we will actually get as a frequented patterns all database entries. That is the same as actually looking at the database, trying to search for that pattern manually.

  For us, support can be set by the user. Since there are now two different algorithms for searching for frequented patterns (one through projects, the other through risks), we decided to have a separate value for each of these algorithms. Having two of them actually helps by evaluation of each approach, because we can easily make one of the approaches not to find anything (setting support to impossible value like 2).

- **Confidence** is a value, that tell us how often do frequented pattern is together. Confidence actually comes from a different approach to frequented patterns, which is called association rules. There is a strong connection between these two. If there is a frequented pattern (A, B), there are two association rules $A- > B$ and $B- > A$. Having confidence we need to check, that item on the right side is often enough present, when item on the left side is present. There are two main reasons for not using it found while confidence was tested.

  - Firstly the semantics of association rules doesn't comply to the approach suggested. We are trying to find common N-tuples among the database entries. Confidence actually selects among rules those that are very strongly connected. That means if I have 4 different 2-tuples with one of this items common (ie. $(A, B), (A, C), (A, D), (A, E)$), you need to have them all present in all projects to be able to mine all 4 of these rules. Having the same item within many other projects without the other part will render it not identifiable. This problem becomes very urgent, if you think about language problems that were mentioned in 6.3.1. That means if different users use different names for the same thing, using confidence will make the whole data mining approach unusable.
  - Secondly the suggested approach is symmetric. If an item occurs often with other item, the approach should succeed both ways. Generating association rules does

create asymmetry within the frequented pattern, because it is not guaranteed that both tests on confidence among frequented pattern will have the same result. For example having a 2-tuple (A, B) will have different supports for $A- > B$ and $B- > A$ in case the amount of occurrences of A and B differs.

These problems proved themselves so big, that a decision to not use confidence at all was made. This decision might not be the best one, but it increases the amount of successfully found risk items one might forget.

As stated before, there is no need to check, if these frequented already found patterns correspond to risks already identified by the user. Within the process is already hard coded the check for this property. The only thing left is to generate all possible candidates out of them. That is done by simple making a set of all possible risk assets and sources. One more problem was found here that might hinder the use of it. If the user (that happened within the first few projects) uses the same word for a risk source and risk asset, these will get merged at this point, making this information get lost. This is not such a huge mistake, since having the same word for a source and asset at the same time, is more or less a mistake of the user. The program avoids this by identifying word phrases as soon as they are written, giving the user hardly any time to change its belonging asset or source. There is though a way to produce this situation. The process to achieve this is pretty simple: just create a new risk in asset tree and a different one in source tree and name them both the same. This will give you the choice to set the word you type in freely between the asset and source you created.

There is usually a test for uniqueness, to make sure no duplicates were found. We need to go one step further and make check, if these items were already identified as assets or sources. The need comes from the point that our approach is symmetric, so it finds the original words as well.

These parts of risk will be used as „whispering“. That means the user will see them while performing risk identification. It is still up to the user, whether to use them or not. No check is being done on that base, to make it easy for the user to evaluate (or add) other projects.

6.4 Qualitative and quantitative risk analysis

Once the user is happy with all the risks that were identified within the first phase, we can continue the process of risk management with risk analysis. The proposed approach was to go through analysis using questionnaires. As proposed in 5 there will be three different values within this process.

- Risk assessment from team performing risk analysis.
- Risk assessment from experts (or simply stakeholders).
- Risk assessment value computed from database.

The first two values have been found to be redundant. The analysis will be performed either by the risk team, by the stakeholders, or both at the same time, making no difference between an opinion of member of risk management team and others. So only one value will be the result of the analysis, which will be compared with the value taken from database.

One thing mentioned before in 5, is that for us there is no difference between quantitative and qualitative analysis. Qualitative analysis is only a disguise of quantitative analysis, so that you can use verbal values instead of exact values. This approach is something we would like to try to avoid, since there is no need to lie to ourselves about it. It is up to everybody to be precise and state values according to his best knowledge.

6.4.1 Questionnaires generation

The first step is to create the actual questionnaires. The pattern of questionnaires was copied from the norm [5], from its normative part (appendix A). The questionnaires are generated according to the asset or source tree, so that they are structured in such a way. There is a big difference between what assets and sources were identified for the whole project, and those which actually appear on the questionnaire. A source or asset will appear only and only then on the questionnaire, if there is a risk that contains it. This has been done according to the problems stated in 6.3.2, where the solution is to create assets that are identified, but have no risks attached to it.

For the generation of questionnaires is the tree-like structure of data used. User has option to choose, which tree is to be used as base (sources or assets). Information from the other tree won't appear in the questionnaire. The program goes through the selected tree and attaches risks to nodes of the tree and thus generates the complete questionnaire. This form has been created printable, to allow the user to hand it out among the team. In case paper evaluation has been used, all questionnaires are gathered and saved into the program.

If the risk management team decides to perform different type of risk analysis, only one questionnaire is filled. This questionnaire is filled with output values from the other approach used, and thus directly translates this information into the database. Since no questionnaires are stored into the database, it doesn't matter, after the project is over, whether there was only one questionnaire fulfilled, or many. The only value that is stored is the final value.

6.4.2 Questionnaires evaluation

Once a questionnaire is fulfilled, it is showed in the list of all questionnaires. It has its own *id*, and together with this *id* a summary of the risk is showed. The summary is counted on a simple basis:

$$summary = probability * (money\_cost + (time\_to\_money\_ratio * time\_cost))$$

User can change *time_to_money_ratio*, so that it follows his project guidelines. If user is thinking about recounting time into money, he should be advised that this is not the simple value that comes from contract (delay in delivery often follows penalty). It might incur even more money to hire extra workers to fix the problem, or buy it from business competition. On the other hand, delay doesn't always need remedy in case there are time buffers for the work to be performed ready. So the user should choose average value of it. He can also try to adjust it in the program a few times to see, which value fits his purpose most.

When more questionnaires are done, they are together evaluated to get some kind of representative value. This value is based on all the questionnaires. User has optional choice on which base to evaluate these questionnaires. There are currently three statistical methods implemented to help the user choose the appropriate one.

- **Mean** is a value normally people call „average“. It is counted: $mean = (\sum_{n \in samples} n)/N$, where N is the number of samples.
- **Median** is said to be the middle value of a sorted set.
- **Mode** is the most common value. If there is more values with the same number of occurrences, the lowest one is used.

Values that come from evaluation of all questionnaires are considered results of quantitative analysis and are then used as final values.

6.4.3 Data mining

There were some database approaches suggested to help the user find the appropriate values for each risk. These values are not considered the best ones, but should only represent some kind of database knowledge. It should give the user some insight about how close is he to those values that are stored in the database. During tests were some features and some drawbacks of these approaches identified. We will go through each of these and discuss them closer.

- **Neural network** was implemented as first one. A simple feed-forward network with 1 hidden layer was implemented, as it is considered the most basic approach. Back propagation was used to learn the network. Artificial neurons with step transfer function were used. To give the reader some insight into what was expected from the network, we should specify the inputs and outputs. Inputs were binary coded asset and source id. These id range from 11024 so 10 input neurons for each of these variable. There were 50 neurons in the hidden layer and 20 output neurons. These output neurons represent the binary value of what was expected. Output was then counted as $decimal\_representation/10$ which makes it possible to reach values $0 - 104857$. No higher values were present in the input examples.

  Test with neural network unfortunately showed that this approach is completely wrong. Neural network gives output value for each input. That is pretty good, but it is semantically wrong to predict something the program doesn't know about anything at all. When a very similar project was done with almost the same risk, this approach showed similar values. Apart of that the values were in average 50% away from the values expected.

- **Linear regression** wasn't implemented at all. There was a simple analysis done through the data gathered and no linear dependency was found. Anyway a simple try with excel (can compute linear regression) showed that this approach would have had even worse outcomes than neural network. On those three (very different) examples it was average 65% deviation.

  Deeper tests were necessary to identify the problem. Linear regression was tried in 3D world. One axis was source id, second was asset id and expected result was probability (later on time and money values). Linear regression tries to match a line in the space for all the risks. This line varies quite a lot, because it plays not only with one variable (preferably with the one we are searching for), but tries to match all points. Having data fairly well distributed among sources and assets makes this approach unstable.

  As is demonstrated on the picture 6.5 with only 4 pieces of data, linear regression can find two very different lines to match the data supplied. The problem is also that

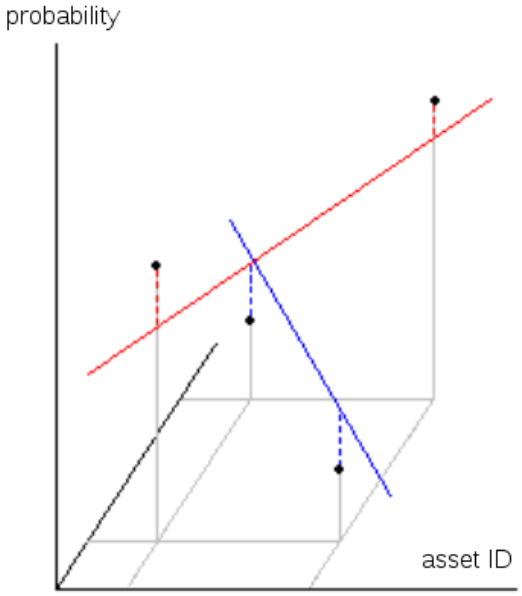


Figure 6.5: Two possible outcomes from linear regression

there is only one dimension that the data can be matched into, making it impossible for two risks next to each other with very different database values to have a very different outcome.

- **Average value** is probably the simplest method to show the knowledge in database. We simply find risks theirs assets and sources match exactly the one we search for and compute an average value from them. Even this value is still not a good one. Added value to this approach is to actually show the number of matches found within the database. That already makes this number worth something. This very simple method still has some drawbacks that lead us to the next approach.

- **Combined value** is a value that not only matches exactly the risk sources and assets, but it takes in account similar risks as well. That means we are searching not for exact match, but for at least one match (either asset or source). That creates an area of risks that we rely on. This method can be compared to clustering method (trying to find similar vectors in space). We just try to find these risks not by position, but rather by assets and sources. The output value is an average of the collected values. For the output value is also very useful to know the amount of risks taken in account.

There is one common problem that has been identified for all of the approaches tried. This problem is in inequality of projects. Each project has a different budget. If the budgets are different, so will be risks. Even for the same risks we might expect the values range dramatically. That is why none of these approaches gives an authoritative answer on how much the risks are.

6.5 Plan risk responses

Risk response has been changed most dramatically during the development. A 3D engine was built for planning risk responses. The biggest problem I have encountered is that it is almost impossible to combine movement along the cube and selecting risks. Selection of risk is done by simply clicking on the bubble representing a risk. This bubble gets bigger and shows all its information. The problem starts when we would like to select a different risk. There are three approaches I tried:

- Rotate around the (0, 0, 0) coordinate. That is the bottom corner of the cube. This showed that it is almost impossible to select one of the risks that are furthers from the bottom. At the same time setting the distance of cutting plane (some objects are not visible although they are in front of camera, but are too close) makes a huge difference. Controlling this approach from user side was not intuitive at all.
- Rotate around middle of the cube. This approach proved itself better, but similar problem arises when the user tries to select a risk that is close to the middle of the cube.
- Last try was to create a full 3D game engine. The user will float through the air freely, being able to move as a „spaceship“. This was very nice but made the use of it very slow.

All three of these approaches had the same problem, which is that the user looses any overview he might have had. The user has to focus more on selecting the risks, than on actual risk response planning.

Because of the problems stated before, a simple list is shown instead. This approach is the simplest one and probably the best one so far. Risks in the list were only sorted according to the risk value, so that the user sees the most important risks first and focuses more on them.

6.6 Project evaluation

A final stage of the project is to gather all information and present the user with the output of the risk analysis. It shows the user the common statistics with some features of how the project looked before and after risk analysis.

- **Number of assets, sources and risks** that are identified within the project.
- **Complete risk summary** of the state before. That means the maximum value of risk before risk responses were set in place.
- **Cost of risk responses** gives us a value, which we need to add to the project budget as money spend. It shows us how much we actually need to spend on preventing risk.
- **Expected residual risk** is the average value that is left after risk responses were put in place.
- **Maximal residual risk** shows us what happens, if everything that can go wrong goes wrong. This might be pretty frightening number in case we have some risks with very high impact, but very low probability and decide to accept them.

- **ISO 27001 compliance** shows whether the project adheres to the norm we set ourselves a goal to achieve ([5]).

These numbers are presented for the control of the whole project. There should be a big difference between the complete summary of the project and its maximal residual risk, otherwise there is a high risk we actually spend more money on preventing risks, than we win by doing it.

Chapter 7

Tests and results

Two stages of testing were suggested. First stage will be filling the database with data and thus creating the knowledge of the database. These projects should be well prepared and professionally performed. Second stage is to create new projects and try to evaluate the efficiency, with which the program helps.

7.1 Test design

Firstly we need some projects that are professionally performed. With the help of the supervisor we decided to use some freely accessible checklist from the INTERNET. Having them from different sources helps keep the variety of the database wide. There were 8 candidate checklists selected for this purpose. These checklists can be found at [16, 20, 19, 15, 12, 18, 17, 13]. While inputting each of these checklists we traverse through these checklists and translate each point into risk and identify its asset and source. One should mark that the sentence we will input into the program is not the same as the item on checklist, because it needs to be reformulated as risk. At some points, one has to artificially create and add a risk source. Considering further evaluation of risks (quantitative analysis) we simply made a suggestion about how much the total budget of the project is, and from that derived the values that were inputted. The values summarized from database are to see on the picture 7.1.

Once this process is finished, we might actually start testing with projects we create our own. The suggested testing was to have 5 projects done from the author of the program, to find the most important features of the system. These tests should contain approximately 10 risks. With these risks we should have theirs assets and sources identified, and quantitative analysis performed. What we will observe while testing is how many assets and sources were automatically identified, the amount of suggested risk sources and assets, and how many of them were found useful (personal feeling of the author of the test). Later in the analysis we will try to compare the monetary value that is expected with experience taken from the database. Author's roommates did promise to try the tool as well, with one example each.

7.2 Results

The first stage of filling the database was pretty hard. One has to identify all the sources and assets. With more projects stored in the database it is progressively easier to put in other risks, because some of the risks asset and sources will be identified automatically. This

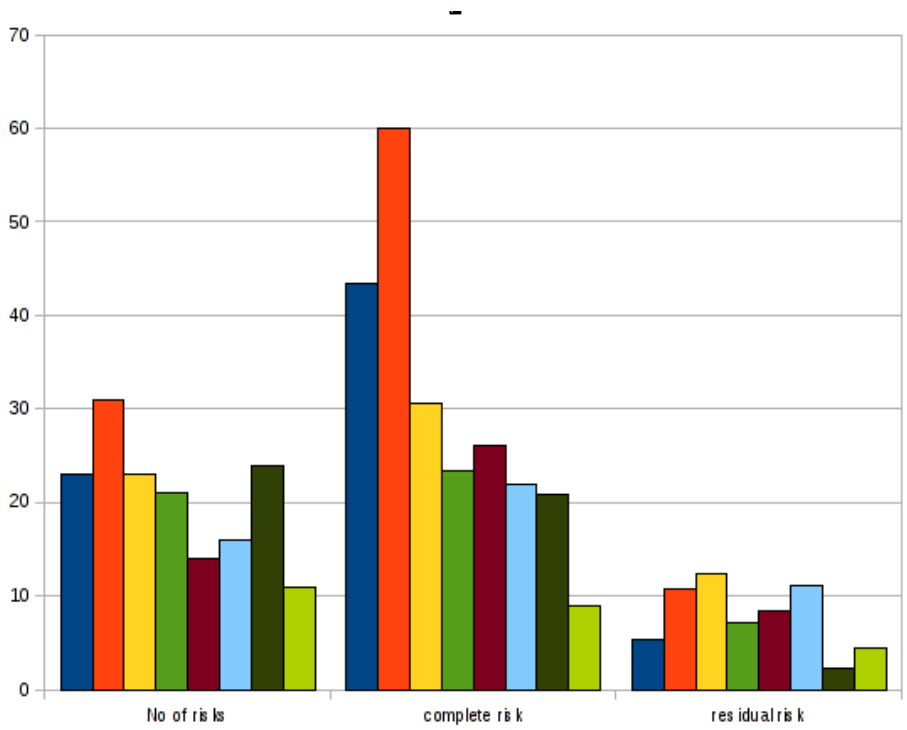


Figure 7.1: Summary of values saved in database (1 risk unit is 500 monetary units)

database is taken as base for testing, where additional projects, that are evaluated, will not get recorded, to make it possible follow at least partially the test again. One problem, that has to be noted, is that even with test not further stored into the database, the monetary value strongly depends on assets and sources that were not automatically identified. This makes it hard to achieve the same monetary results.

On the picture 7.2 we can see comparison of test that were done and their results. According to the labeling we can see which tests were done by Karel Piwko and Lukas Odstrcil. These people (roommates) were chosen as testers. All tests done focus on IT area. One of testers has IT education, the other not. This proved to have no influence on their success in usage.

We could say that this approach is pretty good, because using it will add approximately 65% of other risks that you might have omitted. This might cost you extra money on dealing with them, but usually that is much cheaper than forgetting them.

On the picture 7.3 you can see a typical result of quantitative evaluation of a project. Studies of results showed that there is no dependency between the values expected, and values taken from database. The problem has been already discussed in 6.4.3. So the result from this part is that suggested approach is not very successful one. That means that I found no way to help the user with quantitative analysis based on experience.

7.3 Observations from tests

There were various very interesting observations made that should be noted.

- Sometimes it his hard to draw a line between assets and sources. Some can even be

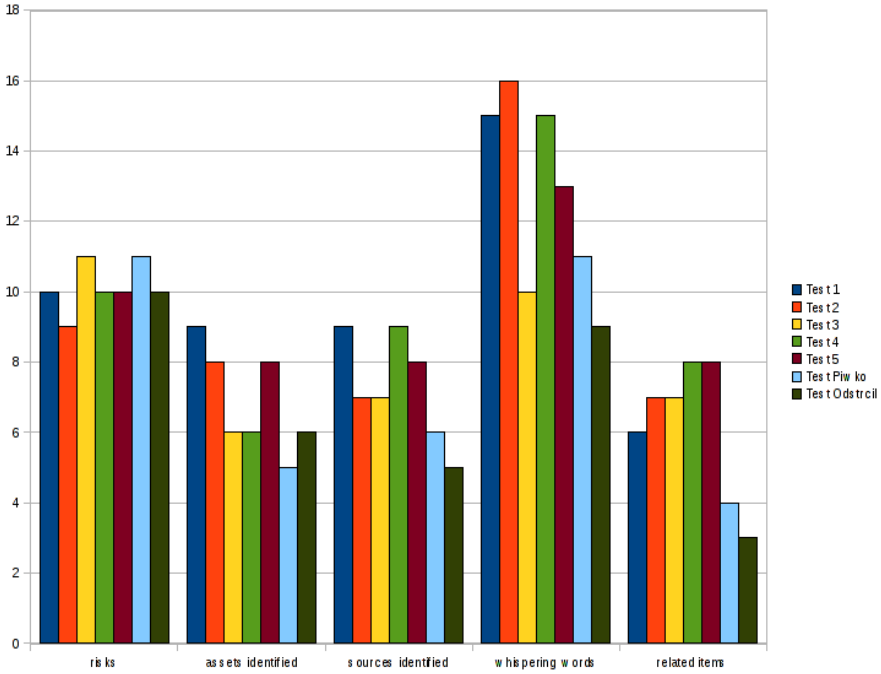


Figure 7.2: Comparison of success

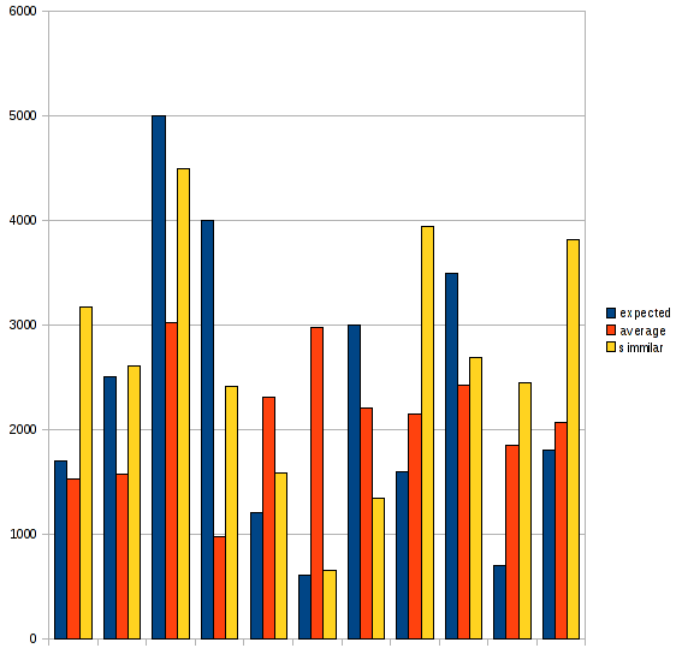


Figure 7.3: Comparison of monetary success

both at the same time. For example employees are not only a valuable asset, but they might create errors as well, making them a source as well. This strongly depends on the user and the way he is used to do risk analysis.

- It would be very useful to integrate spelling check. Since there is a thorough check on word stem, a simple spelling error may render the word unrecognizable.
- There is need for everybody working with the tool, to stick to the same names for the same items. Having multiple names makes problems with similar risks searching and may render the past knowledge unusable. A very useful thing to do, is to create one big tree for sources and assets and have it ready for the user in case he wants to search for a word within the database.
- A very useful feature of the proposed system is that you can use pretty much any language you want even without specific stemming for English. You just need to be consistent in naming things and using exact same word at all occasions.
- Having previous experience about the monetary value of risks stored in the database is not helpful at all. Because projects massively vary in budget, so do monetary risk values.
- We shouldn't check for risks being attached to all sources and assets to make it possible create a asset, that is not applicable to our project, but ISO compliance demands it.

Chapter 8

Conclusion

The main part of this work deals with risk identification. We suggested that data mining approaches can be used to help the user identify risks, he might have omitted. This approach is so far unique and is considered as added value of the author. Experimentally we showed that even a little knowledge in the database helps the user identify about 40% more risks than he would do alone. This is something that we consider a good output, and thus consider this approach valuable. This tool has some special attributes that should be mentioned.

- The system adapts to the user. That means if a single user is using it, his work will get progressively faster and smoother, because most of the work will be done automatically.
- Because the system adapts to the user, it is recommended to have somebody else work with it from time to time, or add a project based on a checklist. That helps keeping up the database variety.
- The tool's performance strongly depends on consistency of naming risk assets and sources.

Second part deals with quantitative risk analysis. All suggested approaches failed to have any reasonable outputs. Using data mining algorithms to support quantitative analysis is thus not recommended. The problem is that budget of projects can vary too much.

This work participated in Student EEICT 2010 conference in the masters section. The project was chosen as second best in its area.

8.1 Future development

There is an approach that the author has found during tests. The approach would be to forget about monetary values of risks, and focus purely on risk identification. It could be done so that we won't try to identify risk sources and assets, but we will go deeply into the language meaning of each word. Once we figure out the basic words (only nouns and verbs), we could consider them as basic atoms of the sentence. All these words will get recorded as parts of risk and the data mining would work on these sets. This way we will make it more transparent for the user (no need to identify any sources and assets), and the result more intuitive (whole frequented pattern as a result - whole part of a sentence).

Bibliography

[1] Kolektiv autorů pod vedením Ing. Jaromíra Pitaše. *National competence baseline of project management*. VUT v Brně ve spolupráci s SPŘ o.s., 2008. ISBN 978-80-214-3665-7.

[2] Gamma, Helm, Johnson, and Vlissides. *Design Patterns*. Cover art, 1994. ISBN 0201633612.

[3] Project Management Institute. *Project Management Body of Knowledge*. Project Management Institute, 2008. ISBN 978-1-933890-51-7.

[4] ISO. *Information technology - Security techniques - Code of practice for information security management*, volume ISO/EIC 17799. pub-ISO, 2005.

[5] ISO. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*, volume ISO/EIC 27001. pub-ISO, 2006.

[6] ISO. *Information technology - Security techniques - Information security risk management*, volume ISO/EIC 27005. pub-ISO, 2008.

[7] R. Pandian, C. *Applied Software Risk Management*. Auerbach Publications, 2007. ISBN 0-8493-0524-1.

[8] Joseph Phillips. *IT Project Management: On Track from Start to Finish*. Corel Ventura, 2004. Book p/n 0-07-223203-X.

[9] WWW pages. Fp-tree based approach for mining. `http://arxiv.org/pdf/cs.DB/0411035`, 20.2.2010.

[10] WWW pages. Morphadorner. `http://picard.at.northwestern.edu/morphadorner/`, 20.2.2010.

[11] WWW pages. Community economic development. `http://www.srds.co.uk/cedtraining/`, 3.12.2009.

[12] WWW pages. Architecture review checklist. `http://www.opengroup.org/architecture/togaf7-doc/arch/p4/comp/clists/syseng.htm`, 3.3.2010.

[13] WWW pages. Checklists: Risk assessment. `http://www.rspa.com/checklists/risk.html`, 3.3.2010.

[14] WWW pages. Decision tree analysis. `http://www.mindtools.com/dectree.html`, 3.3.2010.

[15] WWW pages. Reader-friendliness checklist.
http://www.pantos.org/atw/35317.html, 3.3.2010.

[16] WWW pages. Software accessibility checklist.
http://www.justice.gov/crt/508/archive/oldsoftware.html, 3.3.2010.

[17] WWW pages. Software design document checklist.
http://www.opfro.org/index.html?Components
/WorkProducts/DesignSet/SoftwareDesignDocument
/SoftwareDesignDocumentInspectionChecklist.html∼Contents, 3.3.2010.

[18] WWW pages. Test project setup checklist.
http://bazman.tripod.com/tasklist.html?button5=Test+Project+Setup+Checklist,
3.3.2010.

[19] WWW pages. User documentation checklist.
http://share.skype.com/media/UDC1.0.pdf, 3.3.2010.

[20] WWW pages. Web site usability checklist.
http://www.netmechanic.com/news/vol7/design_no4.htm, 3.3.2010.

Appendix A

Not-ommitable risks

Here is a complete list of not-ommitable risks that fallow the norm [5] appendix A. The structure of the risk is:

```
Name of the risk, ID of the risk, parent ID
```

Thus this creates a tree. The root node of the tree is here marked as root.

```
Security policy, 10, root
    Information, 11, 10
        Security policy, 12 , 11
        Policy review,13 ,11
Information security, 14 , root
    Internal, 15 , 14
        Management commitment, 16 , 15
        Coordination, 17 ,15
        Responsibilities,18 ,15
        Authorization process,19 ,15
        Confidentiality, 20 , 15
        Contact with authorities, 21 , 15
    External, 22 , 14
        customer security, 23 , 22
        third party agreement, 24 , 22
Asset management, 25, root
    Responsibility, 26 , 25
        Inventory, 27, 26
        Ownership, 28, 26
        Acceptable use, 29 , 26
    Information classification, 30, 25
        Guidelines, 31 ,30
        Labeling, 32 , 30
Human resources, 33, root
    Prior, 34, 33
        Roles, 35 , 34
        Screening, 36 , 34
        Terms and conditions, 37 , 34
    During, 38, 33
```

Appendix B

Tests prepared

Name of risk	monetary value expected
There are no text tags for pictures.	4500
There is no contact to be found.	2500
The page doesnt have its copyright and manufacturer signed.	1800
The page doesnt warn you while leaving secure area.	5000
Links are broken.	1600
Links are misleading.	2500
The web can be easily attacked by hacker, because of bad policy.	8000
It is not clear whom is the text suitable for.	1200
The text is inappropriate for the user.	2800

Table B.1: Web design case

Name of risk	monetary value expected
Page is too large to scan read.	700
There are links that are broken.	200
The page is not loaded because no Java is installed.	700
Loading of the page takes too long.	600
The server that host us is attacked by a hacker.	1500
There is no online documentation.	150
Google doesnt mark our page too good.	1500
Some users have different resolution on their monitors.	1200
No sound is played because they have no stereo.	400
There are colors the user cannot distinguish.	50

Table B.2: Web design case

Name of risk	monetary value expected
The server side is not secure enough.	1700
Not only authorized personnel is allowed on the premises.	2500
The operating system is too old.	5000
The operating system has vulnerabilities.	4000
There is no backup of the server.	1200
Patches applied are not compatible with all application.	600
Network is too slow to handle the load.	3000
Virus attack comes through mail.	1600
The standard encryption is not safe enough.	3500
Not all application can be administered distantly.	700
Administrator looses his password.	1800

Table B.3: Server case

Name of risk	monetary value expected
The documentation is too long for user to read it.	3000
Examples within documentation are not well specified.	2000
Documentation of the specific thing doesnt reach the user.	3200
Integration with other application doesnt work out.	7500
User computers are too old to handle the program.	4000
The product needs sound and there is no installed.	1200
The user doesnt understand navigation within the product.	3500
No printing is available.	7000
The program doesnt support local alphabet.	1200

Table B.4: Programming an application

Name of risk	monetary value expected
Product creates too big load for the network.	250
Product is too complicated for the user.	500
Product is not suitable for the user.	600
Data used are already too old.	750
The user doesnt understand documentation.	150
GUI is not very intuitive for the user.	250
There are no text substitutes for visual parts.	200
There is no support that the user may reach.	450
The programmers create too many errors.	800
The product is not well specified.	300

Table B.5: Programming an application