IT outsourcing:  
Risk management by process improvement  
* A supplier oriented perspective *

Nikola Mirkovic  
Master Thesis Information Sciences  
Faculty of Sciences, Vrije Universiteit Amsterdam  
October 2007

**Supervisors**  
Ir. Ton Tijdink MSc. (DNV-CIBIT)  
Prof. Dr. Chris Verhoef (VU)
Management Summary

IT outsourcing deals are uncertain and risky, so organisations need risk management to deal with the high risks involved in these deals. The focus of this research project is on the viewpoint of the IT supplier since much of the research is client focused. A literature study and case studies are conducted in this research project. Three case studies are performed by conducting interviews among five large IT suppliers. Risks derived from these case studies are analyzed and mitigating actions are defined according to the proposed risk framework. The eventual goal of this project is to identify, analyse and mitigate the main risks for suppliers related to each phase of IT outsourcing deals. By doing so, recommendations are given to the Software Engineering Institute (SEI), several IT suppliers and DNV-CIBIT.

From the literature study a proposed risk framework is constructed by combining the CMMI for Development and CMMI for Services models, which are based on process improvement. We conclude that there is no process area for selling services and developing contracts, this indicates a shortcoming of the CMMI models. In contrast, the client oriented CMMI for Acquisition, does contain process areas that describe contracting procedures with suppliers. A change request is submitted to the SEI that contains a recommendation to extend or add a new process area to the CMMI Services.

From case studies, we identified, analyzed and mitigated the main risks. The most risks occurred in project management, and sales contract and development activities. We conclude that the risks from literature and case studies match. The risk framework is not only suitable for identifying risks, but also for mitigating them by assigning practices to the risks from the risk framework. Specific and generic practices are assigned as mitigating actions for main risks identified at case study companies.

We recommend Blue Company to mitigate the main risks in change management and project management by implementing practices from the proposed risk framework. Yellow Company is recommended to implement practices from the proposed risk framework to mitigate main risks during the development of requirements and the pre-contract development. Green Company should focus more on testing risks and implement practices from verification and validation process areas. DNV-CIBIT is suggested to extend its assessments with the risk framework to consult organisations in proactively identifying, analyzing and managing their risks.

Further research should extend the risk framework with process areas in sales and contract development. More and diverse case studies should be conducted to obtain more generally applicable results.
Parties involved

Author: Nikola Mirkovic (1417002)
E-mail: nikola1984@hotmail.com

Institute: DNV-CIBIT
Prof. Bronkhorstlaan 10 X-II
P.O. Box 2
3720 AA Bilthoven

Supervisor: Ir. Ton Tijdink MSc.
E-mail: ton.tijdink@dnv.com

Institute: Faculteit der Exacte Wetenschappen
Vrije Universiteit
De Boelelaan 1083
1081 HV Amsterdam

Supervisor: Prof. Dr. Chris Verhoef
E-mail: x@cs.vu.nl
Preface

While I had to choose a subject for my thesis for the Master program Information Sciences, my interest increased in IT outsourcing. The growing publications on outsourcing got my attention and I decided to contribute to an underexplored aspect of IT outsourcing literature. A lot attention is paid to the client organisation, so investigating the viewpoint of the supplier would have more potential for adding value to the IT outsourcing domain. Since suppliers are exposed to risks and many risks are involved in outsourcing deals, I chose to add a risk management aspect to this subject.

Acknowledgements

First I would like to thank: Ton Tijdink, Chris Verhoef and Wouter Raemaekers for reviewing and providing suggestions. Further many thanks to the experts of DNV-CIBIT, because they brought me in contact with the case study organisations. At last but not least, I would like to thank the participating organisations for providing me information and allowing me to interview them.
IT outsourcing: Risk management by process improvement

Contents

Management Summary ............................................................................................................ ii
Parties involved ........................................................................................................................ iii
Preface iv
Contents v
1. Introduction ....................................................................................................... 7
   1.1 The organisation ................................................................................. 7
      1.1.1 DNV-CIBIT ................................................................... 7
   1.2 List of case study companies .............................................................. 7
   1.3 The business problem ......................................................................... 8
   1.4 The research problem ......................................................................... 9
   1.5 Relevance of project and stakeholder analysis ................................. 10
2. Conceptual research design............................................................................. 11
   2.1 Theoretical approach and focus ........................................................ 11
   2.2 Research goal .................................................................................... 11
   2.3 Research model ................................................................................. 12
   2.4 Research questions ............................................................................ 13
   2.5 Description of concepts .................................................................... 13
3. Technical research design ............................................................................... 15
   3.1 Research material .............................................................................. 15
   3.2 Research strategy .............................................................................. 16
   3.3 Applying the research strategy in 4 phases ......................................... 16
4. Literature ......................................................................................................... 18
   4.1 Defining IT outsourcing ................................................................. 18
   4.2 The evolution of outsourcing and IT suppliers ................................. 18
   4.3 Which services do suppliers provide? ............................................... 21
   4.4 Supplier types ................................................................................... 23
   4.5 Key benefits and objectives .............................................................. 24
   4.6 Outsourcing phases and cycles ......................................................... 25
   4.7 Managing risks in IT outsourcing ..................................................... 28
5. Proposed risk framework ................................................................................ 33
   5.1 General concepts of CMMI .............................................................. 33
   5.2 Introduction to a risk framework ....................................................... 34
   5.3 Process Area Categories ................................................................... 35
   5.4 Focus of risk framework ................................................................... 35
   5.5 Risk framework and Sourcing Service Cycle ................................... 37
6. Conclusions from literature ............................................................................. 39
7. Case studies ..................................................................................................... 41
   7.1 Case Blue Company - Input .............................................................. 41
   7.2 Case Yellow Company - Social ......................................................... 44
   7.3 Case Green Company – Connected .................................................. 47
   7.4 Risk identification and analysis ........................................................ 49
   7.5 Action planning ................................................................................. 50
8. Conclusions from case studies ........................................................................ 53
9. General conclusions ........................................................................................ 54
   9.1 Research question ............................................................................. 54
1. Introduction

This chapter contains a short description of the organisation in which the research project is executed, DNV-CIBIT. Further on, we introduce the case study companies. Companies don’t like to discuss their weaknesses and risks, so they are anonymous in this research; that’s why fictive names are used. At last this chapter contains the business problem and research problem where the research setting is given.

1.1 The organisation

1.1.1 DNV-CIBIT

DNV-CIBIT has approximately 70 employees and is a part of the knowledge intensive and risk oriented organisation DNV (Det Norske Veritas). DNV is an international organisation which has 7,000 employees in 100 countries. DNV-CIBIT has three fields of expertise: Knowledge Management, Information Management and ICT. The vision of DNV-CIBIT is: Global impact for a safe and sustainable future. DNV-CIBIT also offers educational programs like workshops, Master of Science programs and Master Classes.

The project is executed in the field of expertise named ICT. ICT advisors assist customers in: developing and improving IT architecture, performing IT assessments (software product quality), assessing and improving IT processes and improving IT security. Another service offered by ICT advisors is advising companies in outsourcing projects. ICT advisors are advising IT outsourcing companies by assessing the quality of the products and measuring the quality of processes.

1.2 List of case study companies

We provide a list of the case companies, containing a basic overview of these companies. Eventually five of the following (seven) companies are selected for case studies. They all have one thing in common, they provide services in outsourcing.

Atos Origin

Atos Origin is an international IT service provider with 9,000 employees in the Netherlands and 50,000 worldwide. Atos Origin delivers a broad variety of services such as: consulting, developing and implementing IT systems, integrating applications and infrastructure, maintenance and service management. By interconnecting these services Atos Origin is able to deliver full life cycle management and provide services for outsourcing projects.

Ordina

Ordina is a Dutch service provider which is specialized in business units: outsourcing, consulting and ICT. Ordina mainly operates in The Netherlands and Belgium and has 3500 employees in total. Ordina provides services in the following area’s: Enterprise Solutions,
System Integration & Development, Application Management, Technical Automation and Infrastructure Solutions.

**Cap Gemini**

Cap Gemini is an international consulting organisation that also delivers IT services. It has more than 59,000 employees and operates in 30 countries. Cap Gemini provides 3 main IT services: Consulting, Outsourcing and Technology.

**IBM**

IBM is an international computer technology and consulting organisation with more than 355,000 employees and operates in over 170 countries. IBM offers systems integration, hosting, application and consulting services, furthermore it sells software and hardware. From application to infrastructure outsourcing to business process outsourcing services are provided.

**TietoEnator**

TietoEnator is formed by the combination of a Finish and Swedish organisation. TietoEnator is active in close to 30 countries and has 16,000 experts. The services provided by TietoEnator cover consulting, application management, application development, system integration and outsourcing.

**Getronics PinkRoccaide**

Getronics PR has 10,500 employees in the Netherlands and is part of the international organisation called Getronics, with a total of 24,000 employees in 25 countries. The services provided by Getronics PR are: workspace management services, application services, technology transformation services, communication services, security services and outsourcing.

**Logica CMG**

LogicaCMGs services and solutions exist of consultancy, design, systems integration and value-based outsourcing. Its an international organisation with 40,000 people across 41 countries.

**1.3 The business problem**

One of the strongest and most sustained trends over the last ten years has been a move towards outsourcing (Fill, Visser, 2000). IT suppliers and outsourcing companies expect to have advantages like increased availability of resources, higher quality of services and focus on core competencies. But there is a great amount of projects where these advantages are not reached. Some organizations that outsourced their activities ten years ago are now considering to insource these activities. This is not very unusual since half of IT outsourcing projects fails, because of several reasons (Dun and Bradstreet 2000; Hall 2003; Gartner 2003; Deloitte 2005). The possible reasons for this failure: unclear expectations of
outsourcing companies, poor communications and poor performance or quality of IT providers (Taylor, 2006).

It is important to realize that IT outsourcing often is a difficult and complex process therefore it is associated with a high amount of risks. Identifying and mitigating these risks is often crucial to the success of an outsourcing deal, for this reason the demand for IT risk audits is growing.

Most of outsourcing organizations depend on a significant amount of their IT processes but do not have the know-how in-house, so they often outsource these processes to IT suppliers. An IT outsourcing deal consists of a contract between the outsourcing company and the supplier. Many attention has been paid to client oriented IT outsourcing, but much less attention has been given to the viewpoint of the IT supplier. Most research was conducted mainly from the clients’ perspective because the objective of outsourcing is to self-maximize client’s internal resources without taking into account the service provider’s situation (Rao et al. 1996) Since project failures affect IT suppliers too, it is crucial for suppliers to investigate the risks related to outsourcing.

Organizations do not make IS risk management a priority, don’t link IS risks to business strategy, and don’t put enough effort into anticipating problems (Wah, 1999). Therefore risk management can be an extremely powerful approach to dealing with the complexities and uncertainties that increasingly surround technological change and its management (Smith et al., 2001). Risk management has gained more attention since 1980, it evolved from partial risk management to a full grown part of project management and it is essential in identifying and mitigating potential threats.

1.4 The research problem

A number of studies have adopted a risk management perspective to analyze IT outsourcing and have provided useful insights into the phenomenon (Aubert et al. 1999, 2001; Willcocks et al. 1999). These studies investigate risks for outsourcing organizations, but the risks for IT suppliers are under explored. Willcocks and Lacity (1999) state that even though many cases have been researched in outsourcing literature, this has rarely flowed into detailed analyses of risks in IT outsourcing. Outsourcing organizations are minimizing their IT-risks by outsourcing their activities to suppliers, so the risks for IT suppliers are rising. Therefore suppliers are eager to increase the predictability of their outsourcing projects. Applying appropriate risk management is a way to do this.

Outsourcing deals consist of several phases, the general phases are: pre contract, contract execution and post contract. To minimize the risks it is wise to apply risk management throughout all phases of outsourcing. For suppliers it is important to meet the agreed quality of a product or service in every phase. By meeting the quality through every phase of outsourcing, suppliers decrease the chance of a failure.

Integrated Capability Maturity Models (CMMI) are released by the Software Engineering Institute (SEI) which are used by suppliers in order to improve their processes and deliver higher quality. CMMI for Development (CMMI Product Team, 2006) is developed to
address development and maintenance activities. This model is used to identify the process and product risks associated with outsourcing. Another model that is suitable for identification of risks is CMMI for Services (CMMI for Services Team, 2006), it covers the activities required to manage, establish, and deliver services. The more an organization carries out these activities, the more risks it mitigates. By doing so an organisation can reach a higher level of CMMI.

From the research problem the following question can be derived:

*What are the risks and the mitigating actions for IT-suppliers throughout the whole outsourcing cycle?*

### 1.5 Relevance of project and stakeholder analysis

This research is interesting for DNV-CIBIT for two reasons. The first reason is that most of DNV-CIBIT’s current customers in outsourcing are IT outsourcers rather than IT suppliers. By increasing DNV-CIBIT’s knowledge about the outsourcing perspective of the supplier, the range of its customers can be expanded. The second reason is that this research contributes to DNV-CIBIT’s knowledge concerning risk management. Since DNV is risk oriented it would be interesting for DNV-CIBIT to increase its knowledge about managing risks. By doing so, DNV-CIBIT is able to broaden its service offer. This research is the starting point of the contribution in risk management to an assessment method such as the Assess2Improve method (Clerc, Niessink, 2004). This contribution in a risk management approach can also be used by other companies as well, especially the IT suppliers from the case studies.

This research project is also relevant for science, especially for business and information sciences. The research contributes to the IT outsourcing domain and the risk management domain. It’s quite innovative because the risks in outsourcing articles and papers are most of the time client oriented instead of supplier oriented so it provides another view with new insights. Furthermore models such as the CMMI for Services and CMMI for Development are extended, that should be used in risk management studies.

A main problem in business is the IS project failure, solving this requires a proper risk management. The (case study) companies that participate in this research project receive the results of the research that should make them conscious of the risks they are exposed to and which improvement actions can be taken. Especially project managers of service and development departments should benefit of the results of this project, because they have to perform risk management in outsourcing projects.

Finally this research contributes to the researcher’s skills and education. We learned about risk management and outsourcing, and used this information to produce recommendations. Planning capabilities, writing skills, individual working, team working and presentation skills were tested and improved. Eventually this leads to an MSc degree.
2. Conceptual research design

The conceptual research design describes the focus of the research. Then the research model is sketched and the goal of the research is defined. The research questions is derived from the research model and finally a description of the used terminology is given.

2.1 Theoretical approach and focus

The focus of the project is on IT suppliers in outsourcing deals, because this project is considering risks for suppliers rather than clients. Note that these organizations are (former) customers or relations of DNV-CIBIT. For this project we investigated three of five suppliers that were involved in outsourcing deals (see the “List of case study companies” chapter). Further on, we only concentrate on onshoring; off shoring is taken out. This means that we will only consider suppliers and deals in the Netherlands, because we want to compare these companies and deals equally in a limited amount of time. So we won’t consider long term outsourcing such as outsourcing of departments and whole business processes.

The first four steps in the DNV risk management (see Figure 10, Chapter 4.7) approach are mainly considered, from initiation to action planning. Initiation and focusing exists of defining the purpose for risk management. After the initiation step, the identification can be done; risks are identified and organized. The analysis of risks describes how goal achievement is influenced. Then action planning is done where mitigating actions are described. At last the actions are executed in the implementation step. The implementation is out of scope, because implementing risk actions requires for every company tailor-made actions and this is time consuming.

The CMMI for Services and CMMI for Development models as introduced in the research problem, consist of several process areas (PA). By implementing these process areas an organisation can improve its processes. These models contain five maturity levels and the focus is on the first three levels. By selecting relevant process area’s in outsourcing for suppliers, we are able to derive weaknesses and convert them to risks. Although a lot of major risks are derived from the CMMI models, outsourcing literature is also consulted to get a more complete view for our risk framework.

Further on, this project is limited to qualitative risk analysis; quantitative risk analysis is not done because of lack of statistical data.

2.2 Research goal

The goal of this research project is derived from the research problem and the theoretical approach and focus. The goal of this project is to identify, analyse and mitigate the main risks for suppliers related to each phase of outsourcing projects. By doing so, recommendations are given to suppliers for mitigating these risks. This is done by qualitative
identification and analysis of risks in IT supplier companies and the existing literature. Further, recommendations to DNV-CIBIT and scientific research are provided.

2.3 Research model

The research model that is used in this project is illustrated in Figure 1.

To understand this model a stepwise explanation is given. A literature study of risk management and risks in outsourcing is conducted (a). From the literature study a risk framework is derived containing a categorization of outsourcing risks (b). A number of case studies (three) are described by doing interviews among DNV-CIBIT’s experts, customers or their relations (c). From these case studies risks and the way organizations perform risk management in practice are recovered (d). Risks and risk management in theory and practice are combined to perform risk analysis and to assign mitigating actions (e). Finally the goal of this project, recommendations for risk management (g), is reached by combining the risk analysis and mitigation actions with the validation of experts and case study providers (f).
2.4 Research questions

From the research model, goal and focus the following main research question is derived (the questions that belong to the steps of the research model are related to each question):

- What are the risks and the mitigating actions for IT-suppliers throughout the whole outsourcing cycle? (g)

In order to answer this question the following sub questions need to be answered:

- What is IT-outsourcing and which outsourcing life cycles exist? (a)
- What is risk management and how is it related to IT outsourcing? (b)
- Which risks or risk frameworks concerning IT Suppliers can be derived from the existing literature? (c)
- What are the main risks for IT-suppliers in case studies through several phases in outsourcing projects? (d)
- Which models can be used to analyze risks? (e)
- Which mitigating actions can be related to the defined risks? (e)

2.5 Description of concepts

In order to understand the meanings of the concepts and terms that are used in this project, definitions are necessary.

Outsourcing

A business practice in which a company contracts out all or part of its IS operations to one or more outside suppliers. (Hu et al., 1997)

IT

IT (Information Technology) refers to anything that is related with managing and processing information, such as hardware, software and networking.

IT supplier

Any IT organisation that provides IT outsourcing services. Service providers offer a wide array of services such as project management, software development and systems support and maintenance (Currie, 2000). All other common used terms such as third party, vendor, provider or insourcer are identical to this one.

Client

Any organisation that transfers its in-house IT activities to an IT supplier. Another term with the same meaning is customer.

Risk
An unwanted event that occurs with a certain probability and that has consequences towards
one or more goals.

*Risk management*

We will use the following definition of risk management partially derived from (Smith et al.,
2001): risk management is a forward-looking activity that makes the potential risks visible. It
is a formal process by which risk can be brought under control and whereby surprises are
minimized.
3. **Technical research design**

The technical research design provides a description of the required material for answering the research questions. A research strategy is presented to show how the research is performed.

3.1 **Research material**

The main research question is: *What are the risks and the mitigating actions for IT-suppliers throughout the whole outsourcing cycle?* We deal with this question by using as much as possible sources of information so source triangulation is fulfilled. The main question is answered by using diverse sources and methods by applying these to the subquestions:

- **What is IT-outsourcing and which outsourcing life cycles exist?**
  
The main sources that are used for this question are scientific papers and articles (literature). This is necessary to gain insight in the field of outsourcing in a scientific context. Literature provides existing theories and definitions which are useful for the introduction to this research. Media from the internet is used to get an overview of actualities concerning outsourcing. This is needed, to prevent having an outdated research. The media and literature are obtained through qualitative content analysis.

- **What is risk management and how is it related to IT outsourcing?**
  
The same sources as used in the previous question apply to risk management, because there are a lot of theories and models concerning this concept. One source that is added to this question is documentation. Since DNV is a risk oriented organisation it provides much internal documentation like handbooks and methods to deal with risk management.

- **Which risks or risk frameworks concerning IT Suppliers can be derived from the existing literature?**
  
The same sources are used as for the previous sub question; in addition DNV-CIBIT’s consultants are interviewed. These interviews are unstructured with open-ended questions because they are used to orientate on the models used inside DNV-CIBIT.

- **What are the main risks for IT-suppliers in case studies through several phases in outsourcing projects?**
  
The new source types that are used for this question are customers and relations of DNV-CIBIT. Face-to-face, semi-structured interviews with open-ended questions are held with these customers or relations. This is an important method for this
research because it’s used to identify the risks that are occurring in real projects. Other sources are websites of the organisations or the annual reports.

- Which models can be used to analyze risks?
  The already mentioned sources are used to obtain information about risk analysis. Literature and documents are used because there are existing and available methods for analyzing risks.

- Which mitigating actions can be related to the defined risks?
  To obtain the mitigating actions of certain risks literature are combined with validation of persons. The mitigating actions are more justifiable when they are created from different sources.

3.2 Research strategy

A combination of three research strategies is applied to this research project: case study, fundamental theory and desk research. The project will concentrate on a qualitative approach, because we want to give an in-depth view and analysis of main risks in outsourcing.

3.3 Applying the research strategy in 4 phases

1 Literature study

This phase is done by a literature study and interviews. The main goal of this literature study is to derive a risk management framework for suppliers in outsourcing. Furthermore the various services offered by suppliers and supplier types are investigated. To acquire additional information about outsourcing deals and risks, experts (of DNV-CIBIT) are interviewed. These interviews are unstructured with open-ended questions because they are used to orientate on subjects like outsourcing and risk management.

2 Case studies

After risks from interviews and literature study are identified, case studies are conducted. Three customers or relations (suppliers) of DNV-CIBIT are interviewed in order to define and categorize risks. An exploratory case study with a minimal variation is done. Exploratory because risks had to be explored and were not known yet. The minimal variation in cases means that all suppliers are large IT organizations, provide application or infrastructure outsourcing services and we don’t take offshoring projects in account. The only notable variation between these cases is that the suppliers offer different services or products. The method for this comparative multiple case study is hierarchical instead of sequential. We want to compare these cases independently and then do an analysis to get an in-depth view of main risks. We chose a case study for another reason; a case study is a field research and it gains more acceptance in DNV-CIBIT, because of its practical nature.
The interviews are semi-structured with pre-defined questions about risk management, risks and process areas that are carried out in outsourcing deals. Questions are open ended to ensure the interviewee does have enough freedom to provide in-depth knowledge about risks.

3 Analysis and mitigation of risks

The answers to the questions from the case study are used to analyze risks by categorizing them in process areas and to come up with mitigating actions. The results are validated by experts from DNV-CIBIT and case study organizations.

4 Recommendations

In this step, results of the research are summarized and a comparison is made, then recommendations are given. This is done by the research strategy named fundamental theory. A comparison is made between the different cases and the occurring risks and mitigating actions. The recommendations can be used in further research, by the IT suppliers or by DNV-CIBIT.
4. Literature

4.1 Defining IT outsourcing

An organisation that doesn’t want to use its internal sources for IT activities can hire an external company that provides IT services. The definition for IT outsourcing that is used in this research project is: a business practice in which a company contracts out all or part of its IS operations to one or more outside suppliers (Hu, Saunders, and Gebelt, 1997). So outsourcing involves an agreement between a supplier and buyer where the supplier takes over a part of an organisation. Many variations in outsourcing definitions exist, but the differences between them are subtle. There are however various types of outsourcing such as offshoring, onshoring, nearshoring and insourcing. To get an overview a short explanation is given of these terms. Note that these terms are valid in the context of this context.

- **Offshoring** involves outsourcing activities overseas to a country such as India, to lower the costs without sacrificing the quality.

- A relatively new term is **nearshoring**, it involves the same benefits as offshoring but the location of the outsourced activities is geographically nearer than an offshore location.

- An alternative to offshoring and nearshoring is **onshoring**. Onshoring involves outsourcing of activities to areas in the same country as the customer is settled.

- **Insourcing or backsourcing** involves the opposite of outsourcing, it is the continued using of internal resources after the outsourcing option has been evaluated or a previously outsourced activity is been taken in house.

4.2 The evolution of outsourcing and IT suppliers

Outsourcing started back in the early 1960s although the term was rarely used. A more common terminology in those years was facility management, which refers to the operational level of outsourcing (Earl, M.J. 1991). Facility management referred to technology oriented operational services, involving responsibility for the infrastructure (mainframes and network) and the software of these machines, almost no additional services such as consultancy were provided. In the 1980s IT outsourcing became a more mature market. The main reason for outsourcing in this period was cost savings (Takac, 1994). For this reason many IT providers won outsourcing contracts by lowering their prices.

Until the 1990s three types of IT suppliers existed: systems houses that supplied and developed software, IT consultancies that offered diverse services and hardware suppliers (Currie, W.L., 2000). During the 1980s many new IT suppliers entered the outsourcing market and the competition was high. Several reasons for this development are described by Currie (2000).
One reason for the evolution was that the law was changed in the US and UK in the late 1980s by introducing Compulsory Competitive Tendering (CCT). The local government was required to subject more of their public services to competitive tendering. These services may be provided by the in-house department or a private sector organisation depending on the winner of the bid (tender). This led to new outsourcing opportunities for IT suppliers who tried to differentiate themselves by offering software development and application management services.

Other reasons for the evolution of IT suppliers are increased global competition and economic recession. The demands for new services and products where rising in the 1980s that has led to services in various markets like oil gas, financial and manufacturing. IT suppliers developed core competencies in these industries in order to assure long term customer relationships so they could generate higher margins from outsourcing contracts. To expand their reach large suppliers like IBM and LogicaCMG entered strategic agreements or took over other suppliers to satisfy the clients growing demand. In their turn, clients were able to grow faster if they had a contract with a large supplier, because they didn’t have to focus on the IT functions but only on the core business. This was a change in business strategies of many organisations; the focus was on fewer activities (Peters & Waterman, 1982).

Figure 2 Growth of outsourcing deals (Weakland, 2005)

By the end of the 1980s an economic recession hit a great part of the world. Many companies wanted to cut their costs after the recession and this has led to increased outsourcing of IT and business processes like HRM. Partly because of the economic recession managers were more cautious and considered software in-house development as a high risk. So IT suppliers saw the opportunity to offer specialised services such as business process outsourcing and CRM services. A technological reason for the world-wide IT service offerings was that the client-server technology offered many opportunities in contrast to the
mainframes. The computing environment could be distributed geographically; this boosted the globalisation in the 1980s.

Figure 2 shows a result of research done by Weakland (2005) and provides an overview of the worldwide growth of outsourcing deals. A small decrease in outsourcing deals is seen by the end of 1980s because of the economic recession, but it is clear that outsourcing deals since then tremendously have increased. Exact statistics on outsourcing deals are difficult to collect and compare, but this study shows the increasing interest in the phenomenon.

In 1989 Kodak made an agreement with IBM, which would take over the work of four data centres and 300 employees of Kodak. (Applegate, L., Ramiro M. 1995) No company of Kodak’s size had ever turned over its computers to an outsider before. This practice introduced the word “outsourcing” and it became suddenly a seriously strategic choice for large companies.

During the 1990s ERP systems where making entrance into outsourcing. ERP systems can be configured to integrate with information based processes of the client. This gave the opportunity to customers of not developing an entirely new system but integrating already

Figure 3 Development of outsourcing (Gartner, 2003)

existing modules, so implementation times were shortened. Because of this development the globalisation continued and large-scale outsourcing deals were becoming common.

Figure 3 shows different technologies that influenced the outsourcing market as discussed previously. The shift from decentralised services to remote computing caused by the internet had a major influence on the outsourcing services in the 21st century. The internet enabled customers to buy applications on a rental basis. Small and medium enterprises (SME’s) entered the outsourcing industry because they were able to buy affordable software and support from the Application Service Providers (ASP’s). Instead of installing applications
locally, ASP’s offer customer organisations the possibility to access applications over the internet.

With the change of technologies also strategies of the customers changed. In the earlier years cost reduction was the main driver for customers to outsource, but later on outsourcing was seen as a strategy to improve the business. In the 21st century speed to market, scalability and flexibility are emerging as drivers for outsourcing.

4.3 Which services do suppliers provide?

To provide a clear understanding of IT outsourcing services, a description of outsourcing services is given. Outsourcing of the IT function can be divided into two types; application outsourcing and infrastructure outsourcing.

Application outsourcing

Application outsourcing exists of two general types of activities. The first one consists of application development. Application development is the development or modification of customized applications or packaged applications. Also design, implementation and integration of applications can be classified to application development. At last, the rollout of applications can be part of application development (Sadlowski, 1998). The second activity that belongs to application outsourcing is application maintenance and support. The technical environment and applications are kept up-to-date and operational. Further on databases and other software is managed.

Infrastructure outsourcing

Infrastructure outsourcing exists of several, hardware related IT activities. Managing an infrastructure can be defined as preventative and remedial services that physically repair or optimize computing and communications (Beulen et al, 2005). Technical troubleshooting and hardware warranty upgrades are part of this type of outsourcing, but also the helpdesk (online and by phone) and installation assistance. Further on managing the network including servers and desktops are common activities in infrastructure outsourcing.
Comparing the services

Not only the activities between application outsourcing and infrastructure outsourcing are different but also the characteristics of these services. Application development is mainly project based with an average duration of one year (Beulen et al, 2005) while managing services (e.g. infrastructure management) is a continuous activity and takes about three years. Another characteristic of application development is a high level of interaction with end-users and the changing requirements (Faraj et al, 2000; Kraut and Streeter, 1995). In contrast to application development requirements in infrastructure management are stable during the contract; requirements only change in case of service disturbance.

The focus on IT services provided by suppliers is depicted in Figure 4. This figure tells us that there is a high focus on application outsourcing, so it suggests that suppliers are investing in their skills and capacity within this service. The focus on infrastructure outsourcing is medium or low, this suggests that there is a shift to application outsourcing. The reason for this shift is the high demand for application management and development from customers.
4.4 Supplier types

IT suppliers see outsourcing as a business opportunity to sell services. Over the years suppliers have positioned themselves clearly and were more specific about their capabilities. To provide an overview of the outsourcing market-place, the IT suppliers can be divided in five categories according to Fitzgerald and Michell (1998).

Hardware vendors

*Hardware vendors* provide mainly hardware products, infrastructure services and maintenance (e.g. IBM). Often hardware vendors have less contact with the business management of the customer, but however have a close relationship with the IT department. Many hardware vendors extended their services to IT consultancy and application development in outsourcing, because of the declining hardware sales in last decades. They have a difficulty with demonstrating objectivity and independence to their customers in consultancy and application development, since they also provide hardware services.

IT consultancies

*IT consultancies* are driven from a business focus instead of a technology focus, although they specialize in IT and project management. They are often large international organisations (e.g. LogicaCMG) that have a lot of highly trained staff, so their advantage is a global reach and plenty of experience. These IT consultancies focus mainly on IT solutions on strategic and tactical levels and less on operational level outsourcing.

System houses

*System houses* provide services such as application development, maintenance and design. They are often not as large as IT consultancies but some have a global reach (e.g. SAP). There is heavy competition in the market system houses traditionally operated in, because of the IT consultancies that were suddenly offering design and development services. But also the hardware vendors had expanded their services to application development. System houses had to broaden their offer by providing outsourcing services and operational IT management.

Generic outsourcers

*Generic outsourcers* perform low value commercial activities such as infrastructure management and building support services like people management (e.g. catering), desktop PC support and cabling equipment. By bundling these services in one contract, generic outsourcers are able to offer low cost services in comparison with IT consultancies or hardware vendors. This category of outsourcers is less focused on IT and has a background in traditional facility management.

Ex-IT departments

*Ex-IT departments* are former IT departments of large organisations (e.g. Kalido from Shell) and have specific technical expertise at the operational level. The services they provide are
hardware management and software development. Ex-IT departments moved into IT outsourcing by specializing in a specific type of outsourcing such as network management. They also have broadened their services by offering consultancy services (e.g. project management).

Figure 5 IT activities and supplier types (Fitzgerald and Michell 1998)

Figure 5 depicts the five supplier types discussed above, the activities they performed traditionally and the widening of their outsourcing portfolios by offering a broader range of services. This development leads to strategic alliances, acquisitions and partnerships because of supplier’s lack of knowledge or resources in other areas of outsourcing. Almost all the suppliers are moving to the consultancy service, this leads to more competition and the need for long-term contracts.

4.5 Key benefits and objectives

The IT function in the client organisation has become a source of competitive differentiation according to Michael Porter (1985). The IT function is connected to a great part of the value chain, which plays a role in the differentiation of services provided by the client organisation. When the performance of the internal IT function of a client organisation is lower than the performance of a function offered by an IT provider, benefits can be obtained.

General interests for the client in outsourcing are: improved performance, cost savings and greater profitability (see Figure 6). By defining benchmarks, contracts and supplier rewards, an organisation is able to have control over an IT supplier. Other general advantages not depicted in Figure 6 for the client organisation are: greater flexibility in technology, focus on core competencies, economies of scale and access to expertise.
IT outsourcing: Risk management by process improvement

<table>
<thead>
<tr>
<th>Buyer (business objectives aligned with supplier metrics)</th>
<th>Supplier (supplier rewarded for increased value)</th>
<th>Joint</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Well-defined objectives</td>
<td>• Service level targets</td>
<td>• Increase value relationship</td>
</tr>
<tr>
<td>• Internal benchmarking</td>
<td>• Financial target costs</td>
<td>• Initiative creation</td>
</tr>
<tr>
<td>• Evaluation rewards &amp; penalties</td>
<td>• Revenue growth</td>
<td>• External benchmarking</td>
</tr>
<tr>
<td>• Control</td>
<td>• Objective evaluation</td>
<td>• Scenario planning</td>
</tr>
<tr>
<td>• Accountability</td>
<td>• Additional profit</td>
<td></td>
</tr>
<tr>
<td>• Cost savings</td>
<td>• Contract extensions</td>
<td></td>
</tr>
<tr>
<td>• Improved performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Improved profitability</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 6 Interests of buyers and suppliers (Tho, 2005)

Obviously the supplier also has benefits from the outsourcing deal. Benefits are derived from the economies of scale, because the supplier has to perform the same activity, additional profit is made for each unit of work performed. This results in major advantages, like revenue growth. By delivering an outsourcing service a supplier is focusing on activities of core competency this leads to improvement of the efficiency of operations. These competencies are defined by Levina and Ross (2003) and include IT personnel development, customer relationship management and methodology development and dissemination. By improving its efficiency a supplier is rewarded by contract extensions and thereby establishes an income stream.

Next to the client and supplier benefits, joint interests and benefits also result from an outsourcing relationship. A benefit from the outsourcing relationship is the obligation (by contract) to both parties to perform external benchmarks. This common obligation motivates the both parties to improve the relationship, initiate new processes and increase value of the common services. Another joint benefit is the availability of resources available to the supplier and client. This benefit leads more flexibility for both parties in the context of rapid development of new people and new systems.

To have a successful outsourcing deal the client and supplier both have to achieve their objectives and benefits. All benefits come with risks, so every benefit is associated with a risk, this is discussed later.

### 4.6 Outsourcing phases and cycles

The outsourcing activities are performed in distinct phases of an outsourcing deal. These phases or cycles are described by several researchers or commercial organisations. To provide an overview of the available sourcing phases or cycles in the literature we made a comparison in Figure 7. Three different sourcing models are used, one commercial from
Gartner and two from scientific literature made by Zeng (2003) and Lacity & Wilcocks (2000).

Figure 7 Comparing sourcing phases and cycles

Although outsourcing activities in most outsourcing situations are general, organisations, researchers and business practitioners still use their own models for describing these activities. A reason for this difference is that relevant phases for an outsourcing deal depend on the situation of the customer, supplier or the viewpoint of a researcher. However, these models provide a reference point and should be used as a starting point of an outsourcing deal.

The main difference between these three models is in the number of phases they use to describe outsourcing. Clearly, Gartner uses four phases in comparison with Lacity & Wilcocks and Zeng, who use six and five phases respectively. The reason for this difference is probably caused by Gartner’s client focus. Gartner’s Sourcing Life Cycle has only one phase after the contract is signed (see Figure 7), while the other two models use more phases to include the supplier activities. We have studied the two non-commercial models and it seems there is a minimal difference between them except for the names of these phases.

A similarity between the three models is the overall focus on client organisations; all models do not involve the supplier in the first phase. This phase contains activities such as: choosing a vision, deciding on which strategy to use and defining the outsourcing options. It doesn’t
seem strange that we didn’t find sourcing cycles or models that are based on suppliers view, because outsourcing is initiated at the client’s side. But to explore the view of the supplier during the whole outsourcing deal, we have combined the models and generated a Sourcing Service Cycle, as depicted in Figure 8, that can be used by vendors.

Figure 8 Sourcing service cycle

Phase 1: Sales

This phase includes general marketing and sales activities initiated by the supplier. These activities are customer acquisition, analyzing and answering Request for Information’s (RFI) and Request For Proposals (RFP). When a supplier receives a RFI, depending on its interest in the deal, a global solution is created. Then an offer is formulated and sent back to the client. The client scores and ranks the offers and sends a RFP to the preferred suppliers. The RFP contains more specific requirements and specifications, therefore a more specific offer is send back to the client.

Phase 2: Contract development

After the client has received the offers, usually a small number (two or three) of suppliers is selected. Then a due diligence is conducted by the supplier to verify all claims and assumptions by for example interviews. The negotiations are often tough battles between the suppliers, but also between the supplier and customer. Information is hidden by both parties and often suppliers over promise, to ensure they win the contract. But after the contract is signed the relationship becomes better (Gottschalk, Solli-Saether, 2006).

Eventually one supplier is selected, a shared understanding of the service is reached and the contract is signed. The client and supplier define the responsibilities, create agreements for services, agree a price and price model. This includes the creation of a project plan and transition plan. A project plan contains: the time schedule, resource estimation, tasks, risks and responsibilities. The transition plan describes all activities in detail that must be performed to accomplish a successful transition.

Phase 3: Transition
This phase requires the highest level of interaction between the client and supplier; it involves the preparation and execution of the deployment of the new service or product to an operational state. The transition phase actually has two sub-phases, the transfer and transformation (WTO, 2006). During transfer, services and resources such as employees are transferred to the IT supplier. The transformation phase includes the adaptation of customer processes and technology to the supplier’s processes and technology.

The clients’ goal in this phase is to establish performance measures, validate the service scope, distribute the contract internally and promote the contract internally (Lacity & Wilcocks, 2000). Although the client is involved in the transition, the activities are mainly carried out by the supplier, because the actual service or product is developed. The transition plan that is created in the previous phase, is used as a guide for this phase and is being executed.

**Phase 4: Delivery**

During this phase the service or product is delivered according to the service agreements. Supplier activities involved in this phase are: operating, managing and maintaining the systems. Furthermore the IT supplier is identifying problems and continuously improving its service.

According to Gartner (2003) and Zeng (2003) the client has to benchmark and measure the operational performance and compare the results with the expected performance.

**Phase 5: On-going or Exit**

When the deal has past the delivery phase, the client has three options: extend the contract, bring IT back in-house (backsourcing) or switch to another supplier. For the supplier this basically means that there is a contract extension or a contract termination.

If a customer is unsatisfied or has other reasons to terminate the relationship, the supplier goes to the exit phase (see Figure 8). In this case the client has to ensure continued operational performance and explore its options when making a new deal. The supplier has to review its investment criteria and may not invest in new assets if the customer terminates the relationship. Eventually the contract is terminated.

If the customer chooses to continue the relationship and renew the contract, the supplier may continue to maintain the previously service or develop another one so the first phase of the souring cycle starts again.

### 4.7 Managing risks in IT outsourcing

In a contract (not outsourcing) situation, risks and operational processes stay at the clients’ side. The tasks and processes are defined and there is a clear boundary between the supplier and client. But in outsourcing deals the boundaries are blurred because processes, people and technology belong to the supplier who is working for the client. Therefore operational risks are also shifted to the supplier. To manage these risks the suppliers need to have an adequate risk management.
Risk management can be addressed by various perspectives, that’s why different definitions of risk and risk management exist. For example, risk is defined by insurance organisations as an expected loss and the probability that represents the odds that an event will occur (Bowers et al., 1986). Other domains such as finance see risk as the variance of the distribution of outcomes. So the risk is measured by the extent of the variability of results.

The risk definition that we will use is described by DNV (Det Norske Veritas): An unwanted event that occurs with a certain probability and that has consequences towards one or more goals.

Risk management can be addressed by various perspectives, that’s why different definitions of risk and risk management exist. For example, risk is defined by insurance organisations as an expected loss and the probability that represents the odds that an event will occur (Bowers et al., 1986). Other domains such as finance see risk as the variance of the distribution of outcomes. So the risk is measured by the extent of the variability of results.

The risk definition that we will use is described by DNV (Det Norske Veritas): An unwanted event that occurs with a certain probability and that has consequences towards one or more goals.

**Figure 9 Risk dimensions (DNV)**

### Risks types

Risks could be classified as speculative or pure risks. Speculative risks are risks that offer gain or loss (e.g. gambling), while pure risks never result in gains and can result in losses. IT outsourcing is only associated with pure risks, that’s why risk is defined by our definition as an “unwanted event”. Figure 9 shows the wide variety of dimensions of a risk. A main distinction between risks that can be made is between external (exogenous) and internal (endogenous) risks. An external risk occurs beyond the control of the organisation and cannot be affected by any actions of an organisation, while internal risks depend on people actions. External risks of an organisation could be the changing market, an earthquake or regulations. Opposed to the external risks, internal risks depend on people’s actions within an organisation. These risks can occur on different organizational levels; from strategic to operational. Risks on strategic level arise when a poor strategic business decision is made and result in, for example a bad reputation. Operational risks are cause from a failed internal processes, systems or people/management. Our risk definition contains the phrase “that has consequences towards one or more goals”; this means that no matter what risk type occurs, they all have an impact on the objectives or goals of an organisation (see Figure 9). Some of these general goals are described in chapter 4.5.
Risk management

To mitigate and manage risks organisations need to understand risks by proactively handling the important risks to achieve the business goals. In order to understand risk management a more detailed observation is needed. There are many risk management and risk assessment models that are created by organisations or researchers. The overall steps of risk management are pretty general, therefore we will use the model created by DNV. Figure 10 shows the main steps in the DNV risk management approach, it is a proven methodology and it ensures all the steps are taken in a structured manner.

![Diagram of Risk Management Steps](image)

In the first step, *Initiation and focusing*, organisational goals have to be identified, organisational processes are described, risk categories are created and a risk management method is chosen. There are a dozen of methods to do risk management, but the main difference is between qualitative and quantitative methods. If reliable statistical data of the risk probability, consequence and costs is available a quantitative method can be used. But if this data is not available a qualitative method can be chosen by defining the probability of a risk in more subjective terms such as low, medium and high. So qualitative methods depend more on experience and expertise of those executing the method. Moreover it is also possible to combine the qualitative and quantitative methods.

After the initiation, the *Risk identification* step has to be performed. In this step the risks are described, identified and risks are structured. So the risks that have an impact on the goals are revealed and structured to ensure manageability. The step called *Risk analysis* is concerned with: appointing risks to owners/responsibilities, showing the risk exposure and registering the risks.

After the analysis is done, the next step is *Action planning*. The purpose of this step is to develop an action plan by prioritizing risks and identifying the mitigating actions. This action plan can be used to handle the identified risks efficiently, because it contains mitigating actions. Mitigating actions can be divided in four categories (Hallikas et al., 2004):

- risk transfer
- risk taking
- risk elimination
- risk reduction
Transferring risks from an IT supplier to, for example another supplier, can be done when the supplier taking the risk better can deal with it than the supplier transferring it. Risk taking is the strategy used by suppliers to take a risk of an investment in a client organisation and accepting the loss if the risks occur. Eliminating risks is the strategy to avoid the losses or eliminate the risks by actions, which should be caused during the provision of services. At last it is possible to reduce the losses that resulted from risks by for example developing software in iterations and delivering it in phases.

The last step in this risk management approach, Implementation and follow-up, considers the implementation of the action plan and keeping it up to date continuously. During the steps described above, the communicated risks, actions and other activities are registered and documented.

**Main risks in IT outsourcing**

<table>
<thead>
<tr>
<th>Risk factor</th>
<th>No. of projects in which problem occurred (out of 10 troubled projects)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule and budget management</td>
<td>8</td>
</tr>
<tr>
<td>Vendor staffing</td>
<td>8</td>
</tr>
<tr>
<td>Vendor understanding of requirements</td>
<td>4</td>
</tr>
<tr>
<td>Client expectations</td>
<td>4</td>
</tr>
<tr>
<td>Vendor team morale</td>
<td>4</td>
</tr>
<tr>
<td>Change management</td>
<td>4</td>
</tr>
</tbody>
</table>

Figure 11 Six key risks in troubled projects (Taylor, 2006)

Taylor’s (2006) research indicates the top six risks in troubled IT outsourcing deals, perceived by the suppliers (see Figure 11). Three of these risks were unexpected while the other three were identified at the start of the projects. Even though these risks were identified and managed, they still arose after mitigation.

Poor *schedule and budget management* is seen as the most common risk, it’s also a problem that still occurs after it’s mitigated. Budgets and schedules are overoptimistic, often caused by inadequate presales analysis and results in a shortfall of time or budget.

Another risk that occurs often is also made due to an inadequate presales analysis, it’s the underestimation of vendor skills required to work with technology or the skills required for the extra work involved in the projects. So the amount of *vendor staff* and the knowledge are important factors causing these risks.

Not fully *understanding the complexity of the requirements* by the supplier leads to problems with controlling change requests, because from clients’ perspective, these requests are requirements. If the requirements are not understood, this can lead to the implementation of a packaged solution, instead of a customized solution or even developing a new solution. On
the other side the client often doesn’t understands its own requirements and is not able to formulate them well.

An important risk identified in the study by Taylor (2006), is not meeting *client expectations*. Customer satisfaction is related to functionality and performance of the service or product, but it’s also related to expectations. Clients will be unsatisfied if their expectations are higher then the outcomes, this will have an impact on suppliers’ future business and reputation, because new clients will ask for references.

The declining team morale is typically a risk that is caused by the other risks discussed above, since the performance is bad and the project is running out of time; the team of the supplier can have a lack of motivation.

Problems with *change management* occur often, because outsourcing changes the processes and activities in the client organisation. Employees often resist to this change and this could lead to delays or complaints, so an adequate change management is needed.

A risk that is not depicted in Figure 11, but is seen as the most unforeseen risk in Taylor’s research, is *lack of client trust*. Trust is especially important in development projects with customized software packages, because of the vulnerability and dependence of the client on this product. Trust is related to the perceived success of the project and the level of client trust depends on the past behavior of the supplier.
5. Proposed risk framework

This chapter discusses two CMMI models and introduces the proposed risk framework. The proposed framework is based on the general concepts of the CMMI models and will be discussed in detail. The proposed framework contains generic and specific practices that should be used to mitigate risks in outsourcing deals. Further, the focus of the risk framework is defined.

5.1 General concepts of CMMI

To succeed in outsourcing deals suppliers need to manage and enhance their processes. We found two models for process improvement: CMMI for Development (CMMI-DEV) and CMMI for Services (CMMI-SVC). CMMI stands for Capability Maturity Model® Integration. CMMI-DEV is a process improvement maturity model for the development and maintenance of products and services. While the CMMI-SVC covers the activities required to manage, establish and deliver services. CMMI-DEV can be used for application development and the CMMI-SVC is useful in application and infrastructure management.

Both models are developed by the Software Engineering Institute and use the same general concepts. A general concept is a process area, this cluster contains related practices in an area. CMM-DEV contains 22 process areas, while the CMM-SVC contains 25 process areas. Each process exists of:

- General and specific goals, which are considered important to make improvements in that process area. A generic goal applies to multiple process areas and describes the required characteristics to satisfy the process area. A specific goal also requires certain characteristics but applies to only one process area. The goals can be used to determine whether a process area is satisfied.
- Generic and specific practices to achieve these goals. A generic practice describes an important activity that has to be done in order to achieve the generic goal. Specific practices are descriptions of activities that are important to achieve a specific goal.

Process improvement can be done by using two different representations: continuous and staged representation. By using the continuous representation an organisation is able to select one or more process areas and improve the processes related to it so a higher capability level is reached. Capability levels are used to show the improvement of a single process area, there are six capability levels numbered from 0 to 5.

If an organisation wants to define an improvement path, then the staged representation can be used. The staged representation uses a predefined set of process areas and is characterized by maturity levels. There are five maturity levels: initial, managed, defined, quantitatively managed and optimizing. If an organisation wants to reach a maturity level it needs to implement a set of process areas.
5.2 Introduction to a risk framework

Chapter 4.7 shows that a risk can be viewed from different perspectives with various dimensions. Risk management is about identifying potential risks and mitigating these. The first step in the DNV risk approach, initiation and focussing (see Figure 10) requires an organisation to select a risk management method. Most methods or frameworks categorize, group or structure risks by their related subject such as operational, technical, business or financial (DiRomualdo, Gurbaxani, 1998). But they are rarely grouped by the processes in which the risks occurred. A combination of CMMI-DEV and CMMI-SVC can be used for risk management purposes.

<table>
<thead>
<tr>
<th>Category</th>
<th>Process Area</th>
<th>Maturity level</th>
<th>CMMI-SVC</th>
<th>CMMI-DEV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering</td>
<td>Requirements Development (RD)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technical solution (TS)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Product integration (PI)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verification (VER)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Validation (VAL)</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Management</td>
<td>Organizational Process Definition (OPD)</td>
<td>3</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Organizational Process Focus (OPF)</td>
<td>3</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Organizational Service Management (OSM)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organizational Training (OT)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Project Management</td>
<td>Capacity and Availability Management (CAM)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrated Project Management (IPM)</td>
<td>3</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Project Monitoring and Control (PMC)</td>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Project Planning (PP)</td>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Requirements Management (REQM)</td>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Risk Management (RSKM)</td>
<td>3</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Service Continuity (SCON)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supplier Agreement Management (SAM)</td>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Service Establishment and Delivery</td>
<td>Incident and Request Management (IRM)</td>
<td>2</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Service Establishment and Delivery</td>
<td>Service Delivery (SD)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Service Establishment and Delivery</td>
<td>Service System Development (SSD)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Service Establishment and Delivery</td>
<td>Service Transition (ST)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>Configuration Management (CM)</td>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Support</td>
<td>Decision Analysis and Resolution (DAR)</td>
<td>3</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Support</td>
<td>Measurement and Analysis (MA)</td>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Support</td>
<td>Problem Management (PRM)</td>
<td>3</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>Process and Product Quality Assurance (PPQA)</td>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Figure 12 Proposed risk framework

By joining the two CMMI models, our proposed risk framework (Figure 12) can be used by an IT supplier that develops products and manages services. Appendix 1 shows the purposes of the process areas in the risk framework. When we compare the CMMI models, CMMI-SVC has a broader perspective, because it includes the service management and delivery too.

The CMMI-SVC does not contain the engineering category, but instead it contains the Service System Development (SSD) process area that actually contains summarized and less detailed engineering process areas. Therefore we have excluded the SSD process area from our model. The process management category is also excluded from the risk framework, because it addresses particular organisational processes and issues, while we are studying risks related to outsourcing deals and projects. We do not want to study organisation specific risks, because these risks vary for every organisation, while project risks are more common.
Further only the process areas of the first three maturity levels are included, because no company in the Netherlands has a higher maturity level. Eventually the focus of the model is narrowed to 21 process areas and four categories.

5.3 Process Area Categories

To get a more detailed picture of the proposed risk framework, an overview of the categories is briefly discussed. A category contains a set of process areas.

The Engineering category covers development and maintenance activities. This category is especially important for application developers and system integrators. It contains general engineering terminology and can be used by any technical discipline (e.g. software engineering) for product development. So it supports a product (hardware, software, services) oriented process improvement strategy.

The Project management category covers activities related to monitoring, planning and controlling the project. Furthermore the process areas address activities such as taking corrective actions and managing supplier agreements. This category gives direction in every IT project and is important for every supplier.

The Service establishment and delivery category addresses activities that are needed to manage and deliver a service. Managing requests and incidents is a typical activity in this category. Especially IT suppliers that provide service management are affected by the processes described in this category.

It doesn’t matter what the core activities of an IT supplier are, they all need support. The Support category addresses processes that are covered by the other categories. So this process category relies on the input of other processes and deals with quality and measurement of processes.

5.4 Focus of risk framework

Risks need to be categorized by process area, then they should be analysed and mitigated by using the generic and specific practices as actions. By using this risk framework organisations are able to detect their process related weak spots and improve the processes so risks are mitigated. The risk framework is focussed on process improvement, so the focus is on internal risks, rather than external risks (see chapter 4.7 for risk descriptions).

Figure 13 is used to explain in which situations the proposed risk framework is valid. There is a focus on internal risk so the risk framework cannot be applied to every risk type. Figure 13 shows that weaknesses or threats result in risks. The CMMI models are based on organisational weaknesses that result in internal risks; these risks are mitigated by people’s actions within an organisation. Actions that are within the control of an organisation exist of specific and generic practices in the proposed risk framework. However threats are based on external factors, so they result in external risks. These risks are barely covered by the proposed risk framework and are often related to market trends, legislation, natural disasters
and manmade disasters. An internal or external risk has one or more consequences towards the goal(s) of an organisation.

The terminology of weaknesses and threats is derived from the widely recognized SWOT analysis, which is used for strategic planning and deals with strengths, weaknesses, opportunities and threats. A weakness is described as a limitation, fault, or defect in the organisation that will keep it from achieving its objectives. A threat is any unfavourable situation in the organisation's environment that is potentially damaging to its strategy. The threat may be a barrier, a constraint, or anything external that might cause problems, damage or injury.

The dashed line in Figure 13 shows the focus of the risk framework on internal risks and weaknesses. The line is dashed because it defines a focus instead of a boundary. This means that the framework doesn’t entirely exclude threats or external risks. It means that the specific and generic practices should be used to improve the processes of an organisation and generally apply to weaknesses. The risk framework gives some minimal attention to external risks with the use of specific and generic practices in process areas such as Service Continuity and Risk Management. These specific or generic practices guide organisations by the identification of threats or external risks. However, these practices are limited and generally cannot be applied as mitigating actions, since external risks occur beyond the control of an organisation.

A risk can also be caused by a combination of a threat and weakness; in this case it is partly mitigated by a specific or generic practice. An example of such risk is: not meeting client expectations (see chapter 4.7). By implementing the specific and generic practices, client expectations are met such as the agreed functionality and performance. But if the client has unrealistic expectations, this would be a threat and beyond the control of the supplier.

When analysing risks with this risk framework, a distinction has to be made between weaknesses and threats. All risks that are mitigated by the proposed risk framework are...
caused by a weakness or a combination of a threat and a weakness.

### 5.5 Risk framework and Sourcing Service Cycle

Risks can occur in each phase of the outsourcing deal, so risk management has to be performed in each phase. To see how the process areas of the proposed risk framework cover the sourcing phases, Figure 14 can be consulted. We have mapped the process areas to the Sourcing Service Cycle (see Figure 8) by consulting activities in process areas and by validating the mapping with experts of DNV-CIBIT.

<table>
<thead>
<tr>
<th>Process Area</th>
<th>Sales</th>
<th>Contract Development</th>
<th>Transition</th>
<th>Delivery</th>
<th>Exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements Development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical solution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity and Availability Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated Project Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Monitoring and Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Continuity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supplier Agreement Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident and Request Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Delivery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Transition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision Analysis and Resolution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measurement and Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process and Product Quality Assurance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

= Degree of activities

Figure 14 Mapping process area's to Service Sourcing Cycle
This mapping can be useful in risk analysis by paying extra attention to certain activities in process areas in a particular phase of the outsourcing deal. For example, an IT supplier can pay extra attention to risks related to Incident and Request Management, when activities in the delivery phase are carried out. Also the degree of the activities is illustrated, so the most activities in Project Planning are carried out in the contract development phase such as making estimates and creating a project plan. In the following phases commitment to the project plan has to be obtained so these activities are less intensive. A high degree of activities in the contract development phase can indicate that there is a high degree of risks in this phase related to the Project Planning process area. So more attention to Project Planning risks can be given by assigning these risks a higher probability or likeliness in this phase.

The degree of activities can differ from our mapping across organisations, because they perform certain activities according their own rules. But we have validated this mapping by some experts and it shows a general picture for outsourcing deals.
6. Conclusions from literature

In the first two chapters we have defined outsourcing and described the historical developments in IT outsourcing. This information positions our research in the context of the IT supplier. As is described, the IT supplier market has become very competitive over the years. As the market evolved, five different types of suppliers established their IT activities in outsourcing. The high competition caused a shift of activities and suppliers that where only offering infrastructure services in the early days, broadened their services to application development. Furthermore another development is observed; in recent years more and more suppliers provide service management next to application development. By so far we have answered the first part of the research sub question: *What is IT-outsourcing and which outsourcing life cycles exist?*

The second part of this question (*which outsourcing life cycles exist?*) is answered by the comparison of three different sourcing cycles. The compared sourcing cycles or phases have a common characteristic; they all have a client focussed view. This makes the cycles less applicable to organisations providing services or products, because suppliers perform other activities then clients do. We have developed a five phase service sourcing cycle to shape a context and provide guidance in outsourcing deals. Suppliers have to be aware of the fact that a client can back-source its activities in case of dissatisfaction, that’s why we have included an “exit” step in our service sourcing cycle.

The second sub question is: *What is risk management and how is it related to IT outsourcing?* There is no consensus about the definition of risk or risk management, every field of practice uses its own definition of risk. So risk management can be considered from different perspectives and views. Although risk management has various perspectives and methods, we conclude that it is a forward looking process that has to be done continuously. Therefore risk management has to be done in all outsourcing phases of our sourcing service cycle. Further, the main steps in risk management are described to provide an in-depth view of the risk management process.

Half of outsourcing projects fail, so outsourcing deals are related with high risks. Therefore we have described the six main risks for suppliers and according to Taylor’s research (2006) risks still arose after mitigation. One reason for the reoccurring of risks is inadequate risk management.

To perform risk management, organisations are adapting various risk frameworks or methods. Our sub question refers to such a risk framework: *Which risks or risk frameworks concerning IT Suppliers can be derived from the existing literature?* To answer this question we discussed models for process improvement, CMMI for Development and CMMI for Services. By combining these models we have proposed a risk framework for service provision. Our risk framework helps organisations to identify, categorize, analyze and mitigate risks in a structured way. Risks are mitigated when an IT supplier improves its activities that belong to a certain process area. In this way the proposed risk framework gives a more specific indication which specific or general practices have to be performed in order to mitigate risks. We conclude that the framework is focussed on internal risks, which were...
caused by weaknesses within an organisation. This means that the framework is not suitable for threats that result in external risks.

To analyse risks we have mapped the process areas of the risk framework to the phases of the Sourcing Service Cycle. By using this mapping, IT suppliers can focus on certain process areas during a sourcing phase. A remarkable finding of this mapping indicates that there are hardly any activities of the risk framework in the sales phase. Except for the risk management (and PPQA, because of the presence of risk management) there is no process area for selling services and developing contracts. The consequence for the risk framework is that identified contract or sales risks cannot be categorized in any process area, this is validated by experts of DNV-CIBIT. Therefore we had to add questions to our interview, related to the sales and contract development phases (see Appendix 2).
7. Case studies

It’s difficult to discuss risks without a context so case studies are conducted. The case studies are used to test the proposed risk framework, derive risks and provide context. We sent an invitation (see Appendix 3) to the companies on our list (Chapter 1.2) and five companies were willing to cooperate. The participants were managers and directors and had 9 to 25 years experience in IT related projects. Four males and one female were interviewed in sessions of 1 to 1.5 hours.

Before interviewing the participants, we conducted a pilot by interviewing an expert of DNV-CIBIT in order to refine our questions and receive feedback. We created semi-structured, open-ended interview questions that are mainly based on the process areas of the proposed risk framework. At the beginning of each interview we summarized the context and explained the purpose of our research. We showed the sourcing service cycle (Chapter 4.6) to validate the outsourcing phases.

The risks we derived from interviews were often sensitive information. Therefore the names of the case companies, the interviewees and their clients are treated confidential and anonymous. We assigned to every supplier a different colour and used fictive names for their customers. Note that the colours and names do not have a meaning.

When interviewing the managers and directors we made notes, but didn’t use a tape recorder because we would like the interviewees to feel comfortable while discussing this sensitive subject. Later on the notes resulted in cases and we validated the information by email or phone with the interviewees.

All interviewees provided valuable information, but we couldn’t make cases of two interviews, because there was not enough information. The interviewees didn’t provide us with more information because they didn’t have the information or because of confidentiality reasons. Although we didn’t receive enough information, we used the risks they had identified for our risk framework.

7.1 Case Blue Company - Input

Context

Since the market of Input has become commercial, the daily operations and processes changed so the conventional information systems couldn’t support the business needs anymore. Input had to change the IT and operate it, but it had not enough professionals in house to do this job. The continuity of the systems had to be guaranteed, so Input had to expand it’s IT. Input selected a provider, Blue Company (Blue) because it could provide flexibility of systems and employees, apply a pay per use model and reduce the costs. The contract that was signed will run for a couple years and included for 80% the IT infrastructure, desktop management and application management, while the other 20% included application development. Blue took over the whole IT department that included more than 1000 workstations and more than 50 employees. Blue acquired this contract.
because of several reasons. First Blue wants to continue to provide services in the market of Input, second it wants to expand its activities in outsourcing and third it wants to acquire long term contracts.

**Sales and Contract Development**

In the sales phase Input sent a RFI to 8 providers including Blue. After Input had received the responses, it sent a RFP to Blue and other three providers. Input organized multiple workshop sessions that resulted into more interaction among the providers and provided a clearer view of the demand. The RFI and RFP Blue received contained sometimes incorrect information, conflicting information or lack of information of the existing systems or contracts. Blue estimated the budget by using the RFI and RFP and submitted a bid. A misrepresented RFI or RFP could have the consequence of wrong estimated resources or surprises for Blue. The payment structure contained a fixed price in the transition phase and after the transition phase a pay per use model. The risk for Blue to agree a fixed price is that there has to be negotiated again if additional work is necessary.

Two situations were thinkable for Blue in outsourcing deals. The first one was that Input’s internal processes and systems were inefficient, so there were possibilities for Blue to deliver cheaper and higher quality of services. The second possibility is that a customer such as Input already had efficient internal processes and systems, so in most situations it would not be useful to take over their IT. The first possibility was applicable to Input’s case, although it caused a dilemma for Blue. Blue wanted to serve Input as best as possible, but Input didn’t have its IT in place so it was quite a challenge to provide a good service. Another challenge Blue had to deal with in the sales phase was expectation management. If expectations of the business of Input were not managed well then Input would remain unsatisfied.

Before signing a contract, Blue performed a due diligence investigation. This investigation took a lot of time for Input, because the employees had to be interviewed several times by multiple suppliers. Blue couldn’t validate all the information in the interviews and received subjective information because the interviewees didn’t like to speak about their limitations. This is one of the reasons Blue always has to deal with surprises and unexpected situations later on the project.

Another risk for Blue is that the sales phase remains a commercial process, just like other suppliers Blue emphasizes less negative aspects while positive aspects are more emphasized. Blue had to deal with changes within the organisation (a business unit was added) that resulted in the movement of employees between various departments. This was not told to Input until the contract was signed so it could lead to a bad relationship.

**Service Establishment and Delivery**

After the contract was signed the transition phase started. Immediately Blue was responsible for the infrastructure, but the infrastructure was not changed yet. In this phase Blue had to collect information about the available amount and type of products (e.g. servers) and services. Only after the information was collected Blue could start with the service management. Meanwhile Input could keep Blue responsible for problems, while Blue couldn’t provide an optimal service.
One of these improvements was the movement of the data center. This was also a reason for the outsourcing for Input; since the building had to be demolished (including the data center) all the servers had to be moved to another location. But Input didn’t provide an overview of the dependencies between applications, servers and databases, so Blue had to interview employees and study the system. These activities took a lot of effort and time was lost.

The executives and information managers of Input passed the requirements and demands to the internal IT department that translated them into technical terms or specifications and sent them to Blue. Blue didn’t have direct communication with the executives, so the translation of requirements or demands was incorrect in some cases; this resulted in delays or dissatisfaction of Input.

**Project management**

Capacity management was a challenge for Blue, since the internal cost allocation structure was based per user and not per unit (e.g. gigabytes). The internal departments of Input had different needs and concerns. Departments that barely used the IT facilities such as high speed data connections and a high availability of the helpdesk had to pay more because some other departments wanted to use the IT facilities. This caused a mismatch between the usage and costs and resulted in excess or shortage of the capacity. It was more difficult to manage the capacity shortage than the excess, because in case of capacity excess the unused servers could be used for other projects as well. Blue did not have control over this situation; Input was responsible for its internal cost allocation. Blue could only advise a different cost allocation structure.

To manage the infrastructure Blue uses a custom model that is based for 95% on ITIL, therefore all the processes of Input have to be based on ITIL. Some of Input’s processes were not based on ITIL and had to be adjusted. Furthermore Input didn’t have suitable tools that could be connected to Blue’s tools. These tools had to be customized but Blue doesn’t invest into customization, so Blue used their own standard tools.

Risk management was done by Blue with the support of a review process for bids throughout the whole sales phase. A risk register was maintained and used for mitigating actions. Furthermore a risk management system was used through all phases of the outsourcing deal. Technical and financial risks were identified and evaluated. By measuring the occurrence and impact qualitative and quantitative risks were mitigated.

An issue for the management in this deal was the tension between the project team and IT operators or system administrators. The project team was responsible for the transition to the new infrastructure and systems, while the system administrators were responsible for the daily operations of IT. The transition could disrupt the continuity of the IT system, so the system administrators didn’t always cooperated. Their resistance to change was not the only cause for this tension, other reasons such as the culture and processes (no change management) also contributed to this issue. This issue caused delays and disagreements.

**Support**
Incidents and problems with a top priority are resolved by initiating a root-cause-analysis project. This root-cause-analysis project prevents recurring of incidents or problems such as a major unforeseen problem concerning the change management. Input barely had a change management process. The most changes were communicated through a verbal conversation and only 20% of these changes was registered into a system. This was a surprise for Blue, because they expected Input had arranged the change management process according to ITIL. The RFI and RFP contained some Microsoft Excel sheets but these only contained 20% of the total changes, so there was a lack of information. First Input’s processes had to change, only then the transition could continue. Blue needed to collect information about the already implemented processes and which processes had to be implemented. One of the improvements was to physically separate the account managers and system administrators, because they were sharing the same room so no formal change management process was needed. To solve this issue additional work was necessary and time was lost. By performing the actions, such as introducing new processes, Blue was exposed to the risk of providing a lower quality of services.

In this outsourcing deal Blue had taken over 150 contracts, including (back-to-back) contracts with other suppliers as well, like a supplier of a third party application who also managed this application. Blue classified this application as critical for the business continuity of Input, but the supplier didn’t feel it was critical. This was a risk for Blue, because it was responsible for the overall operation IT, including this application and could be blamed if the application would crash. An additional problem with supplier contracts was the absence of a maintenance contract with a hardware supplier. The risks to delay the project and not solving an incident in time increased because there was not direct support of the hardware supplier.

Results

It was clear that the deal would not be finished within schedule, because of the reestablishment of the change management process. Not finishing in time was not a large issue since this project was not time critical. The complexity of the infrastructure and custom applications caused the need for more IT to guarantee a higher service level. The establishment of a change management process and the extra IT systems caused more costs so the goal of reducing costs couldn’t be realized. In exchange for this costs, higher service levels and a higher flexibility of systems or employees is realized.

7.2 Case Yellow Company - Social

Context

Social, an organisation in the social security sector outsourced its IT department and expected to reduce the costs and higher the quality of operational IT activities. The outsourcing included the application management, desktop management and a data center to Yellow Company (Yellow). Yellow acquired this deal because it was a large outsourcing deal consisting of 400 employees and the deal took more than 5 years. Furthermore Yellow wanted to increase its activities in the social security sector. Yellow sold the data center to an IT supplier that was more specialized in infrastructure management. There are three reasons
for this sale. Yellow wants to focus its activities on application outsourcing (including management and development), it didn’t provide enough capacity for data processing and Yellow couldn’t lower its price in contrast to the other supplier. Next to the sale of the data center, the desktop management contract was sold to another supplier. By participating in partnerships with suppliers specialized in infrastructure outsourcing, Yellow is able to deliver a complete solution to Social.

**Sales and Contract management**

A couple of suppliers were selected by Social and eventually Yellow won the deal. Yellow couldn’t be always honest and open to Social because other providers were competing for the deal too. This is a risk for Yellow because hiding information for Social could lead to a poor relationship.

**Service Establishment and Delivery**

Yellow had to obtain the requirements and translate them to specifications such as availability and performance, while Social expected Yellow to understand “the right” requirements. But Social wasn’t able to formulate the right requirements for the application and this resulted in miscommunication. This is a risk Yellow always is exposed to and difficult to mitigate.

The whole IT department was outsourced to Yellow and the consequence was a more formal communication between employees of Social and the IT department. Before the outsourcing started, an employee of Social could request a change by a face-to-face conversation with the IT department. After Yellow took over the applications, informal communication wasn’t possible anymore, so the way of communication was experienced as not personal. Not only the way of the communication changed but also the attitude of the people working for the IT department, they were no longer an employee of social, but were part of Yellow.

Before the outsourcing, the development, management, testing and acceptance testing was done by the internal IT department. Yellow took over the development, management and testing of applications, while acceptance testing still was done by Social. Social had to provide test scripts and descriptions of the desired results to Yellow. The same problem occurred here as with the requirements formulation; Social didn’t prepare itself for the tests and couldn’t formulate the test scripts well, so there was a chance for Yellow that certain functionalities were not tested (correctly).

To mitigate the risks of not resolving incidents or requests (in time), Yellow created a communication protocol that consisted of recording an incident into a system and sending it to a helpdesk or service team. The helpdesk only identified the incident, while the service team resolved the incident. This solution worked and 80% of the incidents and request was resolved.

**Project Management**

No adequate measures of project progression could cause a late delivery of the system or exceeding the budget. Yellow mitigated this risk by checking the used hours with the
available hours. Furthermore the budget and finance are constantly watched by an independent audit department of Yellow. If the budget was exceeded the audit department had to send a warning to the responsible employees.

Risk management is an integral part of project management and is used by Yellow in every project. Risk management was performed in all the phases of the outsourcing deal with Social, because the environment of Social changed by the years so the risks changed too. A risk profile of this deal was made and meetings were used to evaluate the progress of the projects, but there was no standard risk management method because every project needs a custom risk management approach according to Yellow. A major part of the foreseen risks were mitigated, but there were also unexpected risks.

A major risk was the unclear assignment of responsibilities between Social and Yellow, this resulted in miscommunication. The major responsibilities were defined in the contract but the contract was not always consulted. An example of this problem is the installation of applications by Yellow. Social did acceptance testing, but didn’t prepare the environment for the new applications so the application crashed when it was installed. Although it was Social’s responsibility to do acceptance testing and prepare the environment for the new applications, they thought Yellow would do it.

To maintain the continuity of the applications, Yellow documents 60-70% of the knowledge and the other 40-30% is shared through meetings. If Yellow was not documenting and sharing this knowledge, its business would depend too much on individuals. Despite the effort to document the knowledge, Yellow had to deal with challenges during this outsourcing deal. During the transition some employees left and the knowledge of the processes and software related to a specific system was lost. So Yellow had to examine the processes and the software, this delayed the project.

During establishment of the service Yellow had to cooperate with two other suppliers. An issue was resolving the incidents within a maximum resolution time of one day (24 hour). An incident was reported by an employee of Social, but it was not clear what the cause was. The complaint was send to the supplier of the data center, but after a short investigation it seemed it wasn’t caused there. Then the complaint was sent to the supplier of the desktop management, but this supplier wasn’t neither responsible for the incident. At last, the incident was sent to Yellow while the resolution time already exceeded, so Social was unsatisfied with Yellow’s service. This issue demonstrates a continuous risk that is difficult to manage, because every supplier had a different resolution time. An attempt to manage this risk is to synchronize the contracts of all suppliers and Social, so the maximum resolution time is equal in every contract.

Support

To establish the service management Yellow used the ASL standard (Application Services Library), which mitigated potential risks. ASL describes processes such as incident management, change management and service level management. If Social had a request for change (RFC) it had to be sent by a contact manager to Yellow. This agreed communication protocol was not always used, so there were issues. The executives of Social sent a RFC directly to Yellow, without considering the manager (of Social) that was responsible for
contact and communication. Yellow handled this RFC, but this was against the procedures. This resulted in communication issues, because the contact manager of Social was not informed.

**Results and Conclusions**

Social reduced the costs and received a better service, so the customer was satisfied. This outsourcing deal will finish in time and within budget according to Yellow.

### 7.3 Case Green Company – Connected

**Context**

Connected is a foundation with a database that contains personal information of the Dutch population and is connected to a nationwide network. The personal information is used for analysis by 65 different research institutes that are linked to the network of Connected. Connected selected Green Company (Green) in 2003 to build and manage a system that is based on client-server architecture. The main reason for Green to acquire this contract was the establishment in the Dutch market. Since Green is an international organisation, its goal is to get a larger market share in the Dutch marketplace. This outsourcing contract includes application development and application management. The purpose of the application is to facilitate the communication between the institutions, to provide data storage and to support the daily operations performed by these institutions. By the beginning of 2005 Green finished the development of the application. In the middle of 2005 Green started with the implementation of the application at 65 different institutes. The executed activities were the replacement of old systems, the conversion of data and the implementation of interfaces.

**Sales and contract development**

Connected sent the RFI to seven providers and after the responses Connected sent a RFP to three providers including Green. Eventually Green was selected, not because of its technical solution but because Connected felt a cultural fit with Green. Connected selected also Green because of its willingness to take over about 10 former employees of Connected. This meant that there was a risk for Green to provide a solution that doesn’t fit well, since Connected didn’t use the technical solution as the main criterion.

Green admits they overlooked the complexity of the outsourcing deal. Green had good knowledge of developing client software but it was less familiar with the server technology. This means that Green depended on people’s (technical) knowledge. This outsourcing deal concerned a fixed price contract; so Green depended on the correct estimation of the budget.

**Service Establishment and Delivery**

The customer of Green was Connected, but the 65 research institutes had to accept the technical solution (application), so they were customers too. The consequence for Green was that it had to deal with the requirements of Connected and the requirements of the research institutes that were linked to Connected’s network. These requirements were conflicting or were sometimes totally different among each other.
The difference in requirements was one of the reasons for the development of two versions of the client application. The first version exists of the basic application that enables the research institutions to communicate, retrieve and store the information. This basic application allows more flexibility because implementation of third party applications (add-ons) is possible. The second version of the application provides the full functionality because it supports the daily operations of the institutions. The second version was chosen by 90% of the research institutions.

A problem with the compatibility arose while implementing the client application at different operating platforms. The application had to support all Microsoft Windows operating platforms, including outdated platforms such as Windows 95 and Windows 98. The application crashed on all the Win 95/98 while 35% of research institutions were working with these platforms. This was an unexpected risk for Green and it could result into a major loss of customers, if the application was not accepted. The solution was to offer these institutions an upgrade to a newer operating platform. It turned out to be an acceptable solution, only two institutions didn’t agree to this solution.

To solve incidents Green installed a helpdesk that could be contacted by phone, email or a special website. All incidents were registered so they could be tracked and resolved. Green had only two employees working on the support department, this means that the continuity and availability of the support can easily be disrupted.

Further on, Connected could request changes that resulted to three options. The first option was the acceptance of the request and taking actions to deliver the requested service, because the requested service was already paid by Connected. The second option was applying charges for the actions, because the requested service was not paid by Connected. The third option was a refusal because it didn’t fit into the scope of the system. The risk of the third option is that Green can lose customers (research institutes) since they can chose the basic application (instead the complete application) and let a third party develop the requested services.

This outsourcing deal was seen as complex by Green, to mitigate the risk of complexity Green did a lot of testing. But Green was not familiar with large tests so this was a risk too. To perform the tests well they trained testing persons and used various test protocols. Eventually the system had to be delivered twice after the acceptance tests.

**Project Management**

During the capacity management of the application development, Green had a small team of developers, which consisted of less than 10 people. This setup led to the fact that they were able to make decisions quickly with much flexibility. During the testing phase Green faced resource problems, so more capacity was needed and Green hired more people to finish the job. This effort couldn’t prevent that the application was delivered four months too late.

Green admits it miscalculated the risks in the test phase. Green has a risk management process that consists of a monthly review of risks. The risks in this outsourcing deal were reviewed by the likelihood and the gravity of impact. To do a proper project management and risk management a skilled project manager is important according to Green, otherwise...
the project has a high chance of failure. In this outsourcing deal Green had a skilled project manager who focused on risks and mitigated them.

Since Green did not deliver the hardware in this outsourcing deal, another supplier was responsible for hardware support. Connected paid Green to deliver the hardware support and Green paid on their turn the hardware supplier for the support. But after recalculating the costs Green concluded they could deliver the hardware support to save a significant part of the costs.

There were two other suppliers that had a contract with Connected. The first one delivered trusted third party connections for securing the personal information on the network of Connected. The second one delivered data mining services and knowledge management services. These services were clearly defined in contracts but there was an overlap in other services such as consulting. Green was exposed to the risk of missing revenue because the other suppliers would do the consulting. Another risk was that Green was delivering consulting services while this was the task of another supplier.

Support

To maintain the knowledge and changes in the organisation during the outsourcing deal with Connect, Green had three fulltime technical writers that had a fulltime job of documenting all the knowledge. This is a relative large number of employees compared to the team size of developers (less than 10).This activity had to prevent the loss of knowledge, especially of people that were or are leaving the organisation.

Green did not involve an audit party in this outsourcing deal, but they think it is important to do so. According to Green it is crucial to be more self auditing or to involve an auditor to ensure the process and product quality otherwise Green would trick itself, eventually everything is man made. However an auditor was involved in this outsourcing deal which was hired by Connected. Its role was important because it protected Connected’s interest and advised Green during the whole deal.

Results

This outsourcing deal resulted in a high customer satisfaction, because there was an open dialogue and relation with the customer. The development project did not exceed the budget but it was delivered four months later. Connect didn’t see the late delivery as a major problem, because the project was not time critical.

7.4 Risk identification and analysis

By discussing the cases, we identified risks in outsourcing deals or projects. We have successfully categorized these risks into the process areas of the proposed risk framework. This classification can be consulted in Appendix 5 and Appendix 6. Every risk has one or more owners (such as indicated in the risk analysis step) that could be an organisation or an expert of DNV-CIBIT. Furthermore every risk has a consequence that is derived from
interviews. More then 90% (55 out of 60) of identified risks are a weaknesses or a combination of a weakness and a threat, so they apply to the proposed risk framework.

We added the Process Management category to the classification, because almost every supplier classified risks in the Organisational Training process area. We wouldn’t like to ignore these risks, although they are not covered in our risk framework (for explanation see chapter 5). Further the Verification and Validation process areas are merged in the risk classification because both activities run concurrently, use the same environment and refer to testing.

To get an indication of the number of risks, we identified per category, Figure 15 can be consulted. If risks were identified by two owners, then they are counted twice.

<table>
<thead>
<tr>
<th>Risk category</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project management</td>
<td>17</td>
</tr>
<tr>
<td>Sales and contract development</td>
<td>15</td>
</tr>
<tr>
<td>Engineering</td>
<td>10</td>
</tr>
<tr>
<td>Service establishment and delivery</td>
<td>9</td>
</tr>
<tr>
<td>Support</td>
<td>9</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>60</strong></td>
</tr>
</tbody>
</table>

Figure 15 Identified risks by category

The most risks can be found in the Project management and Sales and contract development categories. Although it doesn’t mean that these risks are seen as most important by suppliers, it indicates that there is a high number of risks in Sales and Contract Development, compared to the other categories.

### 7.5 Action planning

Risks are now categorized by process area, the next step, action planning, is to identify mitigating actions. By discussing some major risks identified in the case studies, generic or specific practices can be assigned to these risks as mitigating actions. These discussed actions are not the only mitigating actions a supplier can perform to do risk management, but they do provide a starting point for mitigating these risks by using the proposed risk framework.

**Case Blue Company**

Two major risks occurred in the Blue Company case. The first was a lack of direct communication with executives so the translation of requirements was incorrect and time was lost. The other risk was the lack of a change management process, so a change management process had to be established and time was lost. The first risk, lack of direct communication, is categorized into the Integrated Project Management process area and should be mitigated by:
IT outsourcing: Risk management by process improvement

- Generic Practice 2.7, Identify and Involve Relevant Stakeholders. This GP covers the involvement of stakeholders such as the executives and refers to project management activities such as communications, requirements definitions and decisions.
- Specific Practice 2.1, Manage Stakeholder Involvement. By performing this SP Blue ensures that the executives are involved and requirements are met.

The major second risk, *lack of a change management process*, is categorized into the Configuration Management process area and should be mitigated by at least three specific practices that describe the basis and establishment of configuration management:

- Specific Practice 1.1, Identify Configuration Items. This SP is implemented by describing the items that have to be configured and assigning responsibilities for these items.
- Specific Practice 1.2, Establish a Configuration Management System. By establishing a system for procedures and tools for accessing change request, Blue is able to register change requests.
- Specific Practice 1.3, Create or Release Baselines. By reviewing and agreeing on a set of specifications related to the configuration management system, Blue defines a formal change management process.

**Case Yellow Company**

A major risk in Yellow’s case was: *Responsibilities between the supplier and customer are not clear and not assigned*. This risk is categorized into the Sales and Contract Development category, but the CMMI models do not provide a process area for this risk. Therefore we cannot assign any specific or generic practice to this risk, but we will however provide mitigating actions found in literature later in this chapter.

We will provide two essential mitigating actions for another common risk that also occurred in Yellows case, categorized in Requirements Development: *The customer isn’t able to formulate the right requirements*:

- Specific Practice 1.1, Elicit Needs. By implementing this SP, not only requirements provided by the customer are collected, but also additional requirements that are not explicitly provided by the customer are proactively identified.
- Specific Practice 1.2, Develop the Customer Requirements. By transforming the needs of stakeholders into customer requirements Yellow will obtain a set of technical and business requirements.
- Specific Practice 3.5, Validate Requirements. Perhaps the most important SP for Yellow, since the customers do not know what they exactly want, it is needed to validate the requirements early in the project lifecycle.

By following the specific practices in the Requirements Development process area, Yellow is able to determine the right requirements through a standardized process, even though the customer doesn’t know how to formulate them well.

**Case Green Company**
The main risk for Green was the unfamiliarity with large tests. Green was familiar with smaller projects and test of applications, but they overlooked the complexity of this outsourcing deal. The application was delivered four months too late, because the application didn’t fulfill customer expectations. This risk is classified into the combined Verification and Validation process areas, because it relates to testing activities. Verification is examining whether the application properly matches the specified requirements, while validation is demonstrating that the application will fulfill its intended use. Green had verified the application so it didn’t crash anymore and it matched specified requirements. But the application still had bugs and didn’t fulfill its intended use so there was a risk in validation. The following actions should be taken to mitigate this risk:

- Specific Practice 2.1, Perform Validation. This SP ensures that Green tests the application, so it performs as expected in the intended operational environment.
- Specific Practice 2.2, Analyze Validation Results. The data from validation tests has to be compared with evaluation criteria and expected results.

By implementing these essential specific practices and other practices related to Validation, Green is able to validate the application and it is more likely that Connect would accept the application.

Mitigating risks in Sales and Contract Development

Figure 15, Appendix 5 and Appendix 6 indicate that there is a high number of risks in Sales and Contract Development. Since the CMMI models do not provide a process area for these risks, literature is consulted. These risks could be mitigated by performing a pre-contract requirements analysis (Taylor, 2006). This activity refers to the collection and analysis of requirements before signing the contract, so the budget and schedule are estimated well. A disadvantage is the high costs involved with the pre-contact analysis when the supplier is not selected.

Another effective pre-partnering approach or mitigating action is separating the sales and contract development of the requirements specification (Jiang et al., 2002). This chargeable consulting activity has advantages both for the client and supplier. Clients do not have to make a full commitment to the supplier and can assess the relationship. Suppliers can broadly examine the requirements while applying charge for this activity.
8. Conclusions from case studies

One of the remaining sub questions is: *What are the main risks for IT-suppliers in case studies through several phases in outsourcing projects?* We answered this question in chapter 7.4 by discussing three cases. Appendix 5 and Appendix 6 show the risks, categorized by process area. The most risks were identified in two process area categories of the proposed risk framework: Project Management and Sales and Contract Development. The process area SAM contributes the most to the large number of risks in project management with four identified risks (from six sources). This kind of risks is typical in outsourcing deals or projects, because suppliers often have to cooperate so they depend on each other. Whether a project is successful or not, depends on the management. The success of a project depends on the management of a project so this type of risk is major and occurs throughout all phases.

Contract and Sales Development risks occur during the first two phases and are important because they have a large impact later on the project. Risks such as incomplete RFI’s and RFP’s or a limited amount of time for due diligence, cause unexpected schedule and budget problems. We have successfully mapped the identified risks to all phases of the service sourcing cycle (Figure 14), so all phases of an outsourcing deal are covered.

The following sub question is answered by literature research and validated by case studies: *Which models can be used to analyze risks?* The proposed risk framework is used to analyze the identified risks in the case studies. We described and classified the risks, identified the consequence, and indicated the owner of these risks. We conclude that the proposed risk framework is useful for risk analysis. However we didn’t demonstrate how to derive the risk exposure. A risk has a certain probability of occurrence, the probability or prioritization of risks is not analysed because this is out of scope of our research.

The last sub question is: *Which mitigating actions can be related to the defined risks?* Chapter 7.5 answers this question by providing specific practices that can be used by the case study companies to mitigate their major risks. We show that the specific (or generic) practices can be connected to identified risks, so risks are addressed by improving certain processes.
9. General conclusions

9.1 Research question

In chapter 6 we answered the first three sub questions by concluding from the literature study. We created a five phase sourcing service cycle to shape a context and provide guidance in outsourcing deals. Further we concluded that risks have multiple dimensions and that risk management isn’t just a chapter in a project plan, but it is a continuous activity. The main steps in risk management (see Figure 10) and the six main risks in outsourcing deals for suppliers are described. We proposed a risk framework by combining the CMMI for Services and CMMI for Development. The risk framework has a focus on weaknesses within an organisation instead of threats. By mapping the process areas of the proposed risk framework to the sourcing service cycle, we showed that there are barely any activities in the sales and contract development phases.

The remaining sub questions are answered in chapter 8 by analyzing case studies. We identified and analyzed the main risks in three case studies. We concluded that the risk framework is applicable in practice for identifying, analyzing and mitigating risks. Further specific practices are used as mitigating actions for main risks identified at case study companies.

The main research question is: What are the risks and the mitigating actions for IT-suppliers throughout the whole outsourcing cycle? By performing the first four steps of the risk management approach (Figure 10, chapter 4.7) we were able to identify the main risks for IT suppliers and recommend mitigating actions. The risks that were found in three case studies are described in chapter 7, the most and major risks are identified in the Project Management and Sales and Contract Development categories. However this does not excludes other major risks in other process area categories, it indicates on which category IT suppliers need to pay more attention.

The six main risks found in literature (Taylor, 2006) correspond to the risks in the case studies. One of the six main risks is poor schedule and budget management, this risk is identified often as a consequence in the case studies. Not meeting client expectations is also identified as a consequence in our case studies. Further, problems with change management were also common and occurred in every case we discussed, especially in Blue Companies case. We expected to find risks in the risk management process area, but every supplier had a standardized risk management process. An explanation could be that we have only interviewed large organisations, which often have a mature risk management process. However, every supplier was exposed to unexpected risks, so risk management has to stay a priority process in these organisations.

To address the second part of the research question “throughout the whole outsourcing cycle”, we added the Sales and Contract Development category to the proposed risk framework, because it didn’t contain any activities in this category. By this way, the proposed risk framework covers the whole outsourcing cycle. We conclude that the lack of sales and contract management process is a shortcoming of the CMMI-SVC and CMMI-
DEV, so we sent a change request form to the Software Engineering Institute (see Appendix 4).

Specific Practices and Generic Practices can be used as mitigating actions for the risks identified in case studies. By implementing these practices suppliers are able to mitigate risks throughout the sourcing cycle, except in the sales and contract development phases. Although we didn’t provide any specific actions for these phases, we did propose some general approaches such as: performing a pre-contract requirements analysis or separating the sales and contract development of the requirements specification. By a separation of the pre contract and post contract activities, suppliers would be able to examine the requirements before signing the contract so there would be fewer surprises after the contract is signed.

9.2 Recommendations

By analysing risks we provided recommendations for the case study companies in chapter 7.5. These recommendations are based on specific and generic practices of the proposed risk framework. By implementing these mitigating actions, project managers of IT suppliers are able to mitigate risks in outsourcing deals. We recommend suppliers to use the proposed risk framework to identify, analyse and plan mitigating actions.

Case Companies

By implementing practices from process areas Configuration Management and Integrated Project Management, Blue Company is able to improve their processes concerning the major risks in the case study.

Yellow Company can implement practices from Requirements Development and pay attention to the Sales and Contract Development to mitigate its major risks in the case study.

Green Company should focus more on the Verification and Validation process areas to mitigate the risks occurred in application testing.

A general recommendation to these suppliers is to prioritize the identified risks by assigning a probability and consequence to each risk. By doing so suppliers should mitigate the most important risks in their organisation. Another recommendation to all suppliers is to be more open to customer organisations in the sales phase; this will often result into more trust and avoid poor relationships. By being proactive in the contract development phase by suggesting a pre-partnering approach, client expectations and requirements would become clearer. More clarity and information would prevent many risks later on the outsourcing projects.

Further, suppliers have to be aware of higher risks caused by the involvement of other suppliers in the outsourcing deal. Partnerships or consortiums between suppliers are formed to mitigate these risks, but suppliers have to be aware of new risks involved in partnerships.

DNV-CIBIT
This research is useful for DNV-CIBIT but also for other consulting organisations. The proposed risk framework is especially useful for DNV-CIBIT, because it adds value to risk oriented process audits.

An assessment method such as the Assess2Improve (Clerc, Niessink, 2004) could be extended with the risk framework and identified risks. We demonstrated how the risk framework can be used to assign mitigating actions; DNV-CIBIT should do this the same way. There is another way to use the proposed framework; when a supplier doesn’t implements a process area, DNV-CIBIT could indicate the risks it is exposed to. By using the risk framework from this view, DNV-CIBIT consults organisations to proactively manage their risks. Further, the risk framework refers to development and service management so it is useful for both types of services.

This research also indicates that there are major risks in sales and contract development; this is a chance for DNV-CIBIT or other independent consulting organisations to acquire outsourcing deals and provide guidance through these activities.

Software Engineering Institute

As we concluded in chapter 9.1, there is no process area that refers to sales or contract development activities. In contrast, the client oriented CMMI for Acquisition (Dodson et al., 2006), does contain process areas (Solicitation and Supplier Agreement Development; Acquisition Management) which are used to describe and manage contracting procedures with suppliers. We submitted a change request form (see Appendix 4) to the SEI, addressing a change in CMMI-SVC. The CMMI-SVC is an initial draft version, while the CMMI-DEV is a full version document, so the change request would more likely affect the CMMI-SVC. Our recommendation to the SEI is to extend the SAM process area because it already contains contract agreement activities, but it refers to suppliers only. The SAM process area could be extended with goals and practices that establish agreements with clients.

Our other suggestion is to add a new process area (e.g. Client Agreement Development), however this requires a more radical change to the CMMI-SVC. This process area should contain the following goals or specific practices: creating a sales strategy, performing due diligence and creating a formal agreement.

9.3 Further research

This research has some limitations that could affect the obtained results. The risk framework is focused on deal or project issues but doesn’t consider organizational issues. A major risk that was identified by three sources is left out: key employees are leaving the organisation. Our focus on project issues could result in a less complete risk picture. Note that the list of the identified risks is infinite so there is no guarantee that the identified risks are the only risks in outsourcing. Further, the risk framework focused on internal instead of external risks. More field research is needed to understand the supplier risks involved in outsourcing deals and more attention has to be given on the mitigation of external risks or threats.
The high number of risks in sales and contract development phases indicates that the complexity of the performed activities is high, probably even higher than in post-contract phases. However, more research is needed to confirm this claim.

To use the proposed framework, basic knowledge about the CMMI models is required. The risk analysis and mitigation depend on the knowledge and experience of the person that performs risk management. For example, if the identified risks are not specific enough, they could be categorized into more than one process area, so it becomes difficult to assign mitigating actions.

The reliability of the results would increase if more participants were involved in the research project. We interviewed five large IT suppliers and some experts of DNV-CIBIT, so our conclusions should be viewed cautiously and may not apply to all IT suppliers. The identified risks apply commonly to large suppliers in the Netherlands, but small and medium enterprises were not investigated. Although this research may not apply to all IT suppliers, it does apply to all supplier types because the case study organisations were different types of suppliers. Further research should concentrate on more and diverse companies to obtain more reliable and generally applicable results.

We treated all results anonymous and confidential to obtain high validity as possible. After the interviews we validated our findings. However, the information is obtained from several participants who all have their own interests, so the information may be subjective. Although the participants remained anonymous, they could have hidden some negative risks or information that could have a negative impact on their reputation. Interviewing more employees of one organisation would have resulted in more objectivity of our research.
# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Due diligence</td>
<td>An investigation, performed by the supplier, to validate and examine all material facts</td>
</tr>
<tr>
<td>RFI</td>
<td>Request for information, is used to gather information (offerings) on products and services from potential suppliers.</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for proposal, is an invitation for suppliers to submit a proposal on a specific product or service through bidding.</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information Technology Infrastructure Library is a globally recognized collection of best practices for information technology service management.</td>
</tr>
<tr>
<td>SP</td>
<td>Specific Practice</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for change</td>
</tr>
<tr>
<td>GP</td>
<td>Generic Practice</td>
</tr>
</tbody>
</table>
Bibliography


Deloitte (2005) *Calling a change in the outsourcing market: The realities for the world’s largest organizations*. Deloitte Consulting.


## Appendix 1. Purpose of Process Areas

<table>
<thead>
<tr>
<th>Category</th>
<th>Process Area</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering</td>
<td>Requirements Development (RD)</td>
<td>Produce and analyze customer, product, and product component requirements.</td>
</tr>
<tr>
<td></td>
<td>Technical solution (TS)</td>
<td>Design, develop, and implement solutions to requirements. Solutions, designs, and implementations encompass products, product components, and product-related lifecycle processes either singly or in combination as appropriate.</td>
</tr>
<tr>
<td></td>
<td>Product integration (PI)</td>
<td>Assemble the product from the product components, ensure that the product, as integrated, functions properly, and deliver the product.</td>
</tr>
<tr>
<td></td>
<td>Verification (VER)</td>
<td>Ensure that selected work products meet their specified requirements.</td>
</tr>
<tr>
<td></td>
<td>Validation (VAL)</td>
<td>Demonstrate that a product or product component fulfills its intended use when placed in its intended environment.</td>
</tr>
<tr>
<td>Project Management</td>
<td>Capacity and Availability Management (CAM)</td>
<td>Plan and monitor the effective provision of resources to support service requirements.</td>
</tr>
<tr>
<td></td>
<td>Integrated Project Management (IPM)</td>
<td>Establish and manage the project and the involvement of the relevant stakeholders according to an integrated and defined process that is tailored from the organization’s set of standard processes.</td>
</tr>
<tr>
<td></td>
<td>Project Monitoring and Control (PMC)</td>
<td>Provide an understanding of the project’s progress so that appropriate corrective actions can be taken when the project’s performance deviates significantly from the plan.</td>
</tr>
<tr>
<td></td>
<td>Project Planning (PP)</td>
<td>Establish and maintain plans that define project activities.</td>
</tr>
<tr>
<td></td>
<td>Requirements Management (REQM)</td>
<td>Manage the requirements of the project’s products and product components and to identify inconsistencies between those requirements and the project’s plans and work products.</td>
</tr>
<tr>
<td></td>
<td>Risk Management (RSKM)</td>
<td>Identify potential problems before they occur so that risk-handling activities can be planned and invoked as needed across the life of the product or project to mitigate adverse impacts on achieving objectives.</td>
</tr>
<tr>
<td></td>
<td>Service Continuity (SCON)</td>
<td>Establish and maintain contingency plans for continuity of agreed services during and following any significant disruption of normal operations.</td>
</tr>
<tr>
<td></td>
<td>Supplier Agreement Management (SAM)</td>
<td>Manage the acquisition of products from suppliers.</td>
</tr>
<tr>
<td>Service Establishment</td>
<td>Incident and Request Management (IRM)</td>
<td>Ensure the timely resolution of requests for service and incidents that occur during service delivery.</td>
</tr>
<tr>
<td>and Delivery</td>
<td>Service Delivery (SD)</td>
<td>Deliver services in accordance with service agreements.</td>
</tr>
<tr>
<td></td>
<td>Service Transition (ST)</td>
<td>Deploy new or significantly changed service systems while managing their effect on ongoing service delivery.</td>
</tr>
<tr>
<td>Support</td>
<td>Configuration Management (CM)</td>
<td>Establish and maintain the integrity of work products using configuration identification, configuration control, configuration status accounting, and configuration audits.</td>
</tr>
<tr>
<td></td>
<td>Decision Analysis and Resolution (DAR)</td>
<td>Analyze possible decisions using a formal evaluation process that evaluates identified alternatives against established criteria.</td>
</tr>
<tr>
<td></td>
<td>Measurement and Analysis (MA)</td>
<td>Develop and sustain a measurement capability that is used to support management information needs.</td>
</tr>
<tr>
<td></td>
<td>Problem Management (PRM)</td>
<td>Prevent incidents from recurring by identifying and addressing underlying causes of incidents.</td>
</tr>
<tr>
<td></td>
<td>Process and Product Quality Assurance (PPQA)</td>
<td>Provide staff and management with objective insight into processes and associated work products.</td>
</tr>
</tbody>
</table>
Appendix 2. Interview questions

General questions
1. Can you name an outsourcing deal or project and discuss it from a risk management perspective? (context, customer, result)
2. Which IT functions are subject of outsourcing in this outsourcing deal and what is the length of the deal?
3. What was the most important reason to acquire this project for you?*
4. In which phase(s) did you perform activities?
5. Does your organisation uses a sourcing cycle and how do you describe it? (show sourcing cycle)

Sales and Dealmaking
6. Which risks occurred during the sales process?
7. What did you see go wrong while making the deal? (e.g. due diligence, doing interviews)

Engineering / Service Estab. & Delivery
8. Which risks did you see in developing requirements from user specifications?
9. Did your organisation make a transition plan and which challenges did you see in the transition phase?
10. Which risks did you see while integrating your service/product with the existing product/service of the customer? (e.g. interface compatibility)
11. Which challenges did you see during the delivery stage? (design, implementation, technical solution)
12. How do you perform incident and request management and which risks did you see in this project?
13. Do you test the work products (e.g. design, prototypes) to see if they match with the requirements and which risks occurred while testing?

Project Management
14. How did you perform capacity management and which risks did you see occurring?
15. How did you carry out project management and which problems did you have to solve?
16. How did you monitor and control your project progress and what can/did go wrong?
17. Which challenges did you see during the creation and maintenance of the project plan?
18. What did you see go wrong while managing requirements (changes in req)?
19. In which phases do/did you perform risk management, which method do/did you use?
20. Which risks did occur but where not mitigated by risk management?
21. What actions do you take to ensure service continuity and what is the biggest risk of service disruption?
22. Which risks did occur when cooperating with other suppliers for the same customer? Or suppliers that only deliver products to you?

Support
23. How did you carry out change management and which risk did you see occur?
24. Did you use a formal decision process and what were the challenges? (e.g. selection of test environments, tools, suppliers)
25. Did you measure for example your data and used it to support management information needs? (such as measuring the performance of system)
26. Did you identify and address underlying causes of incidents to prevent them from recurring? Which risks did occur?
27. Did you use formal methods to objectively evaluate your products and ensure quality? (e.g. by audits of external parties)

**Last questions**

28. What is the result of the project? (customer satisfaction, time, costs)
29. Can I send you some questions via email for clarification?
30. Would you give me some feedback on the case?

* = “YOU” IS EQUAL TO “YOUR COMPANY”
Appendix 3. Invitation to interview

Research project Risks in IT outsourcing:
A supplier oriented perspective

Invitation to interview

MSc Information Sciences, Vrije Universiteit Amsterdam

DNV-CIBIT
Nikola Mirkovic

Introduction
My name is Nikola Mirkovic and I participate in the master programme Information Sciences at Vrije Universiteit in Amsterdam. Therefore I’m performing an internship at the ICT advisory department of DNV-CIBIT (www.cibit.nl), an independent organisation that performs activities in advice and education.

**The context**

One of the strongest and most sustained trends over the last ten years has been a move towards (IT) outsourcing. But there is a great amount of projects where the expected advantages are not reached and projects fail. It is important to realize that IT outsourcing often is a difficult and complex process therefore it is associated with a high amount of risks. So it is interesting to identify these risks and reveal actions that mitigate these risks.

**The goal of the research project**

The eventual goal of this project is to develop recommendations for performing risk management in IT outsourcing projects. These recommendations are derived from risks and mitigating actions found in literature and cases (interviews). The focus of this research is on:

- Project risks of an IT supplier, in particular one project (case) will be discussed
- Onshoring, no offshoring
- Application outsourcing and infrastructure outsourcing, no business process outsourcing

The main research question is: *What are the risks and the mitigating actions for IT-suppliers throughout the whole outsourcing cycle?*

**The research**

For the field research I’d like to interview experienced people working for large IT suppliers in the Netherlands.

*Are you willing to cooperate in this research project and provide some time (1,5 hour) for an interview?*

I realize that the information you provide can be sensitive, therefore your name, the name of your organisation and the name of your clients will be treated confidential and anonymous. I will send you the results (my master thesis) to thank you for participating. In the thesis you can find the main risks in outsourcing projects and which mitigating actions can be taken.

**Contact**

Email: [nikola.mirkovic@dnv.com](mailto:nikola.mirkovic@dnv.com)
Tel. nr: 0640324861
## Appendix 4. Change Request Form, CMMI-SVC

### Initial Draft CMMI for Services

**Change Request Form**

Email completed forms as attachments to cmmi-cr@sei.cmu.edu

Visit www.sei.cmu.edu/cmmi/models/change-requests.html for updates to this information.

<table>
<thead>
<tr>
<th>Name:</th>
<th>Nikola Mirkovic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization:</td>
<td>DNV-CIBIT</td>
</tr>
<tr>
<td>Branch/Department:</td>
<td>ITGS</td>
</tr>
<tr>
<td>Position:</td>
<td>Trainee</td>
</tr>
<tr>
<td>Telephone:</td>
<td>private</td>
</tr>
<tr>
<td>Email Address:</td>
<td>private</td>
</tr>
</tbody>
</table>

**Review Type:** (Select one: Individual Review or Coordinated Group Review)

Individual

**Group Description:**

/

**Element Affected:** (Describe item to be changed, including section name and page number)

Process areas (in case of SAM page 351), specific goals and specific practices.

**Requested Change:**

Extend a process area such as SAM with sales and contract development activities, focusing on the client instead of the supplier. My other suggestion is to create a new process area that deals with sales activities and contract development. This process area could be added to the Project Management category.
**Rationale for Requested Change:**

Service providers are facing high number of risks that often originate in the pre-contract phase of a project. This is the result from my research conducted at five large IT Suppliers in the Netherlands. Therefore they need guidelines to improve the sales or contract development process.

The CMMI for Acquisition (CMMI-ACQ) contains a process area named Solicitation and Supplier Agreement Development (SSAD), which is used in the pre-contract phase to prepare for solicitations, select suppliers and establish supplier agreements. Furthermore the CMMI-ACQ contains the process area Acquisition Management (AM), which is used to manage supplier agreements. But the CMMI-ACQ is focused on the client organisation, instead on the suppliers. It is remarkable that the CMMI for Services (CMMI-SVC) does not contain such a process area and doesn’t describe a contracting procedure with clients. The SAM process area of CMMI-SVC contains contract agreement activities, but it refers only to other suppliers. Therefore it should be extended with goals and practices that establish agreements with clients.

My other suggestion is to add a new process area (e.g. Client Agreement Development) that contains specific goals or practices such as:

- creating a sales strategy
- performing due diligence
- creating a formal agreement

By creating this new process area, suppliers would be able to improve their sales and contract development process in projects. The CMMI-SVC could be used in every phase of a project and the full project life cycle addressed in this way.

---

**Bottom portion of form for internal use by CMMI Steward.**

**Tracking ID:**
Appendix 5. Risk classification 1/2

IT outsourcing: Risk management by process improvement

Nikola Mirkovic

Risk framework

Service Establishment and Delivery

IRM
- Exceeding the maximum resolution time of an incident because of dependence on other suppliers. (Yellow)
- Customer is unsatisfied.
- Communication issues.
- Handling RFC’s of persons that are not permitted to do a RFC. (Yellow + experts)
- Bad performance of service delivery that is not corrected. (experts)
- Contract termination or penalties.
- Preventive maintenance is not done. (experts)
- Costs for maintenance are higher than expected.
- Taking responsibility for problems at beginning of the transition phase (Blue)
- Don’t have the chance to make improvements, so could be blamed by client.
- Less important problems may be solved. (experts)
- Delay in services and decrease in productivity.
- The current/daily operations have to continue while the service has to be transformed to the new situation. (White)
- Disruption of daily operations.

SD
- Let multiple stakeholders develop requirements. (Green)
- Conflicting requirements or requirements that are out of scope.
- Special requirements in functionality. (Blue)
- Delays, implementation problems or contract termination.
- The client has insufficient knowledge of its processes. (White)
- It takes more time to formulate the requirements.
- Customer thinks the supplier is proactive and will find the right solution.
- The customer is not able to formulate the right requirements. (Yellow)
- Miscommunication.
- Dissatisfaction.

ST
- The product applications are incompatible with the clients operating system. (Green)
- Customer refuses the product.
- More time is needed or budget is exceeded.
- The customer doesn’t have suitable tools that could be connected with the suppliers tools. (Blue)
- Delay.
- Overseeing the complexity so a lot of testing is needed. (Green)
- Delay.
- Supplier is not familiar with large tests. (Green)
- More capacity in terms of employees is needed.
- The customer doesn’t prepare itself enough for the tests and doesn’t formulate the test scripts well. (Yellow)
- Functionality is not tested.
- The applications are developed at the supplier system and acceptance testing is done at the customers system. (Red)
- Performance problems.

TS (Technical Solution)
- The customer barely has a change management process so the process has to be implemented. (Blue)
- Time is lost.
- Quality of service is lower during this implementation.
- Absence of documentation of dependencies between applications, servers and databases. (Blue)
- Studying the system takes a lot of effort and causes delays.
- The client wants a research that measures satisfaction or benchmark. (White + Red)
- Costs and barely no advantages for the supplier.

VER & VAL
- Known problems are not solved. (experts)
- Will keep causing incidents.
- Solutions to problems are not made available (experts)
- The resolution costs more time.
- Not involving an objective party so there is a less objective and less critical view (Green)
- Lower quality of product.
- Clients with low maturity (processes are not institutionalized) want to change quickly, but it takes more time to change. (Red + Blue)
- It is difficult to provide the best service to the customer.

DAR (Decision Analysis and Resolution)
- The client wants a research that measures satisfaction or benchmark. (White + Red)
- Costs and barely no advantages for the supplier.

CH
- Absence of documentation of dependencies between applications, servers and databases. (Blue)
- Studying the system takes a lot of effort and causes delays.

MA
- Known problems are not solved. (experts)
- Will keep causing incidents.

PRM
- Solutions to problems are not made available (experts)
- The resolution costs more time.
- Not involving an objective party so there is a less objective and less critical view (Green)
- Lower quality of product.

PPQA
- Clients with low maturity (processes are not institutionalized) want to change quickly, but it takes more time to change. (Red + Blue)
- It is difficult to provide the best service to the customer.
Appendix 6. Risk classification 2/2

Risk framework

IT outsourcing: Risk management by process improvement