Institute of Architecture of Application Systems
University of Stuttgart
Universittsstrae 38
D–70569 Stuttgart

Diplomarbeit Nr. 3538

Risk assessment-based decision support for the migration of applications to the Cloud

Mengjie Sun

Course of Study:	Computer Science
Examiner:	Prof. Dr. Frank Leymann
Supervisor:	Dr. Vasilios Andrikopoulos
Commenced:	July.29, 2013
Completed:	Febuary.24, 2014
CR-Classification:	D.2.1, H.3.3, K.6.5

Abstract

Cloud computing is described by NIST as a model for enabling network access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. With the advantages such as flexibility, scalability and expenditure reduction, cloud computing attract many enterprises to begin to consider the migration of applications into Cloud. However, open issues like cloud reliability, economic requirements, performance goals, compliance enforcement and information safety should be certainly taken into account. In this thesis we focus on identifying and classifying risks with different migration types according to the template defined by IRM, developing a migration support system that supports stakeholders to make decisions before migration applications to the Cloud, implementing the system logic as a set of Web service, and evaluating the system.

Contents

List of Figures

List of Tables

1 Introduction

This thesis is aimed at arranging all the risks that occur by migrating to the Cloud in a template by Institute of Risk Management and trying to implement a decision support system based on risk assessment. The main contents involve the summary of related works, introducing the new catalogue of risk, design and implement as well as the evaluation of a decision support system. In the first chapter the motivation of this work is described, and the scope of problem as well as the outlining of this thesis is explained.

1.1 Motivation

Nowadays cloud computing is a popular topic for blogging and white papers and has been featured in the title of workshops, conferences and even magazines [1]. It also has been under a growing spotlight in both industrial and academic areas [2]. With its scalability, high-availability, flexibility and cost efficiency cloud computing has now emerged to become one of the best solutions for companies who want to revamp and enhance their IT infrastructures. However, many practical experience evidences that there are some certain issues and problems along with these advantages. It is no need to recommend everyone to adapt to this new technology, but it is also wise to recognize the risks associated with the cloud migration, so as to avoid the possibility of future issues. Therefore security becomes one of the most major issues of cloud computing.

Recently many works are concentrated on identifying the risks occurring by the cloud adoption and some organization like National Institute of Standards and Technology (NIST) has already given such a comprehensive analysis of its contexts, likelihood and consequences [3]. While Microsoft has established a mechanism related to this, which is concerning what and where may be happen by migration and how to deal with it [4]. PlanForCloud.com even provides a spreadsheet of risks as the basis of decision making for discussing in an arrangement meeting [5]. On the other side, the Institute of Risk Management (IRM) has defined a risk management standard of how to describe the risks with all the possible information including risk name, scope, nature, stakeholder, quantification, appetite, treatment, improvement and policy development as well [6]. However there are no works yet focused on risks definition of cloud computing by using this IRM standard of risk description since 2002.

At the meanwhile lots of documents such as the research by Ali Khajeh-Hosseini et al. [7] are involved to provide an efficient way to help the user for an overall analysis with benefits and risks, who wants to migrate applications or infrastructures to the cloud. Decision support system has revealed its superiority by offering a direct and visualized

mean for decision maker. So a kind of decision support system based on risk assessment is on demand.

By all accounts, applying the template offered by IRM to identify all the risks by the cloud migration and designing a risk assessment-based decision support system is the initial motivation of this work.

1.2 Problem Definition and Goal

This work aims to set up a new risk catalogue concerning cloud adoption which is based on the template defined by IRM, and then develop a system to provide the user an intuitive mean to understand which risks they may confront with what kind of effects and how to avoid these risks occurring or mitigate their negative consequences, and eventually may help to make decisions. Therefore this thesis focuses on 2 main problems:

1. How to adapt all the risks to the IRM standards of risk description and expand it with all the information needed?
2. How to address risks with considering different deployment models as well as migration types and return all the possible risks to the user in a user-friendly decision support system.

To the first problem, this work is based on a full understanding of IRM standards of risk management and devoted to identify all risks of cloud migration by referencing over 50 scientific literatures and technical reports, and then tried to adapt all the associated information to the corresponding attributes and features of the template of risk definition. To the second problem, massive works has been done to confirm the risks occurrence related to different deployment models and different migration types. Hence a complex database is established to record all the relationships between risks and these models as well as types and some questions are additionally asked for to enhance the accuracy of risk searching.

There are also some technical problems in how to design the system in order to offer a powerful function with a simple interface and convenient operations, and how to set up the data relations in a rational database for a better searching ability and return all the needed information to the users.

1.3 Outline

In this work the following research approach is applied: collecting the related works about cloud migration, risk management and decision support system, developing new risk catalogue, analyzing requirements, designing system, implementing and evaluating the prototype.

This thesis consists of 6 chapters. After outlining the thesis, the fundamentals of cloud computing and cloud migration are introduced in chapter 2. Some decision support systems are presented such as the Cloud Adoption Toolkit from Khajeh-Hosseini et al.

[8] and the conceptual model of decision making for cloud migration by Andrikopoulos et al. [9]. The knowledge of ISO 31000 standards for risk management is also concerned. In chapter 3 we tried to apply the standard of risk description by IRM and developed a full-detailed catalogue of risks by cloud adoption. Chapter 4 explains the requirements and specifications of a decision support system and focuses on the design and implementation of a risk assessment-based system named RaDSuS. Finally the evaluation of this system that is based on use cases related to the migration of exiting application to the cloud is presented in Chapter 6.

2 Background

In this chapter some basic knowledge concerning cloud computing is described first, then some related works about migration are referring to and the template from IRM is introduced and discussed.

2.1 Cloud Computing

Nowadays there is a new trend that more and more enterprises choose cloud computing for IT solutions. Cloud computing is an on-demand service model for IT provision, mostly based on virtualization and distributed computing technologies. It allows the company to get their applications up and running faster, with improved manageability and less maintenance. It also enables IT to more rapidly adjust available resources to match the fluctuating and unpredictable business demand. With the advantages of scalability, flexibility, optimal resource utilization and reduced capital costs, cloud computing get more attention from all trades and professions. Therefore this new economic model for computing has found fertile ground and is seeing massive global investment. According to the analysis from International Data Corporation (IDC), the worldwide forecast for cloud services in 2013 amounts to $44.2 billion, with the European market ranging from 971 million in 2008 to 6.005 billion in 2013 [10].

Cloud computing architectures have many features as following [3]:

- Highly abstracted resources
- Instantaneous provisioning
- Near instant scalability and flexibility
- Shared resources (hardware, database, memory, etc.)
- service on demand
- Programmatic management (e.g., through WS API)

According to the recent established definition by NIST, cloud computing is described as a model for enabling network to access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of three service models and four deployment models [11].

2.1.1 Service Models

Cloud computing providers offer their services with different models: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) where IaaS is the basic and each higher model abstracts from the details of the lower models [12].

- SAAS
  The capability provided to the consumer is to use the providers applications running on a cloud infrastructure. Cloud provides a special collection of software for the consumer to access through a client interface or a program interface. The consumer doesnt need to manage the issues such as software installation, upgrades and maintenance. SaaS is usually referred to web-based software, on demand software, or hosted software.

- PAAS
  Cloud providers deliver a computing platform and a solution stack as a service. It allows the consumer to create the software using tools and libraries, which are offered by service provider, and to deploy applications and configure settings. It is no need for consumer to manage or control the cloud infrastructure such as network, servers, storage and operating system.

- IAAS
  The consumer is provided with all infrastructure components such as servers, network capacity, storage, communication devices, archiving and backup system and other components of data center and network infrastructure from cloud provider. The cloud provider is responsible for housing, running and maintaining the hardware.

With the rapid development of the cloud computing, more models with the key component as the form X as a service (XaaS) were created, such as database as a service, strategy as a service, process as a service, etc. In 2012, communication as a service (CaaS) and network as a service (NaaS) were formally included to the family of cloud computing models by International Telecommunication Union (ITU), which indicates a brilliant and broad prospect of cloud computing.

2.1.2 Deployment Models

Depending on the kind of cloud deployment, the cloud may have limited private computing resources, or may have access to large quantities of remotely accessed resources. The different deployment models present a number of tradeoffs in how customers can control their resources, and the scale, cost, and availability of resources [13].

- Public Cloud
  The cloud infrastructure is provisioned for open use by the general public. It may

be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

- Private Cloud
  The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

- Community Cloud
  The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

- Hybrid Cloud
  The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Considering the security, public cloud has a higher risk associated with data protection, as the data are accessible by the public. In comparison to public, private cloud is an infrastructure solely operated for one organization. The data in private cloud are more secure, since on one apart from the organization has access to it. Controlling over data on community cloud is higher than public cloud and the security concerns are more than the private cloud since there are a number of organizations using the infrastructure. Finally the hybrid model is a combination of two or more public and private cloud with all the risks occurring on these two models.

2.2 Cloud Migration

According to the definition from Techopedia [14]:

> *"Cloud migration is the process of partially or completely deploying an organization's digital assets, services, IT resources or applications to the cloud. The migrated assets are accessible behind the cloud's firewall."*

Cloud migration facilitates the adoption of flexible cloud computing. Cloud migration is so critical, that it will directly influence the future system performance, efficiency and costs, thus it require an explicit analysis, exact planning and execution before migration to ensure the solution on demand.

2.2.1 Application Architecture

Figure 2.1 illustrates the architecture of an application, which can be seen as 3 layers according to Fowler et al. [15]: presentation, business logic and data. In comparison with migrating the virtual machines of applications on IaaS model, PaaS and SaaS offerings of cloud providers enable alternative options of migration for applications, i.e. moving one architectural layer to the cloud instead of the whole application. Furthermore a set of architectural components from one or more layers can also be moved to the cloud with considering different deployment models.

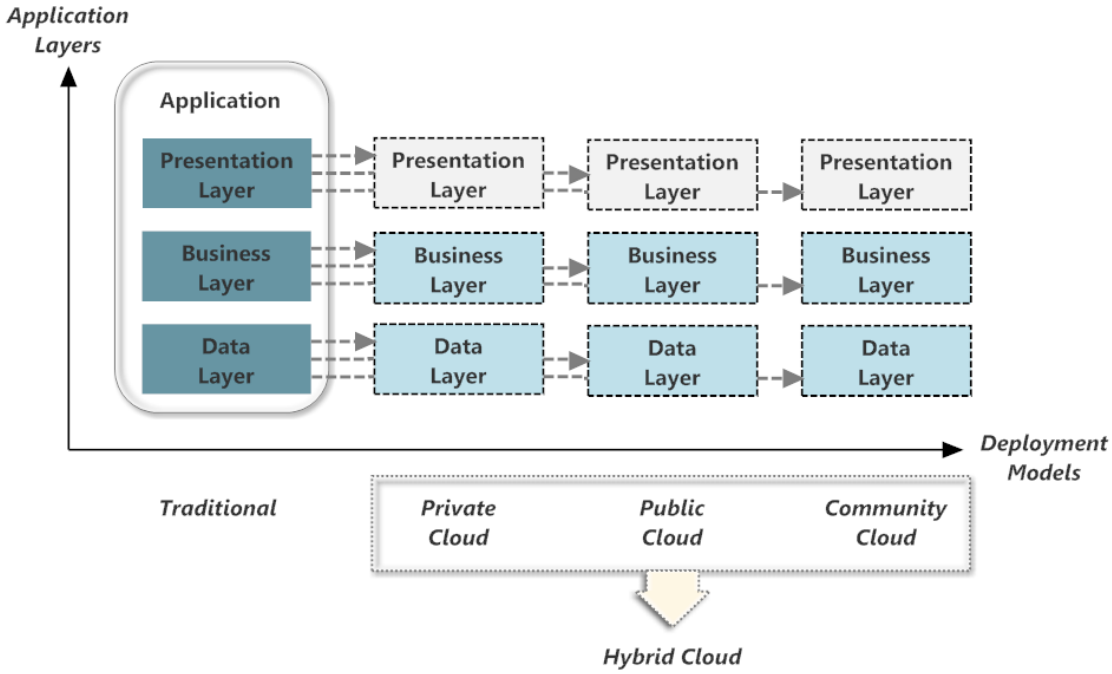


Figure 2.1: 3-Layer-Architecture of Application with Deployment Models and Possible Migrations [16]

2.2.2 Migration Type

In order to distinguish between different approaches of migrating an existing application to the cloud, four types of migration are defined [16]:

- Type I
  Replace one or more (architectural) components to the Cloud, which usually refer to some data and/or business logics. It is the least invasive way of migration with some risks. As a result, a series of activities like configurations, rewriting and adaption will be triggered to deal with the incompatibilities, which may be happened after migration.

- Type II
  Migrate one or more application layers or a set of architectural components, which are interactive and implement the same functionality from one or more layers, to the Cloud. It is so-called partially migration.

- Type III
  Migrate the whole software stack of the application to the Cloud. This is the classic and typical way of migration, by means of encapsulating relevant applications into a number of Virtual Machines and then running in the Cloud.

- Type IV
  Migrate the application completely into the Cloud. That means all the data layers and business logic layer are moved and served as a composition of the Cloud Services, with some adaptive actions.

2.3 Decision Support Systems for Cloud Migration

2.3.1 Decision Support Systems

From the existing works we already know that migrating of applications to the Cloud is a multi-dimensional problem with comprehensive analysis and detailed research, and always with feedback loops as well. To find an appropriate Cloud offering, a series of decisions should be made with considering the relationship and influences between them. Sometimes the system performance may determine these decisions and sometimes budget is a very important consideration, and usually it needs to find a trade-off between the cost estimation and performance expectation. In this sense a healthy decision support system is on demand.

Referring to the research by Andrikopoulos et al. [9] a version of a Cloud migration decision support system is proposed, with considering all aspects above. Figure 2.2 describes a conceptual model of decision support system, which helps the developers and stakeholders to find out whether and how to migrate their application to the Cloud. In this model 2 types of concepts are identified, *decisions* and *tasks*. The *decisions* are the key part of the system, consisting of 4 actions: Distribute Application, Select Service Provider/Offering, Define Multi-tenancy Requirements and Define Elasticity Strategy). Each decision has a direct or implicit influence on the others, displayed with transparent arrows. Additionally 7 *tasks* are identified: Work Load Profiling, Compliance Assurance, Identification of Security Concerns, Identification of Acceptable QoS Levels, Performance Prediction, Cost Analysis and Effort Estimation. These tasks may affect the decisions, illustrated with solid narrow arrows, or vice versa. All the decisions and tasks as well as their relationships and influences constitute a network form for helping to make decisions by migration an application to the Cloud.

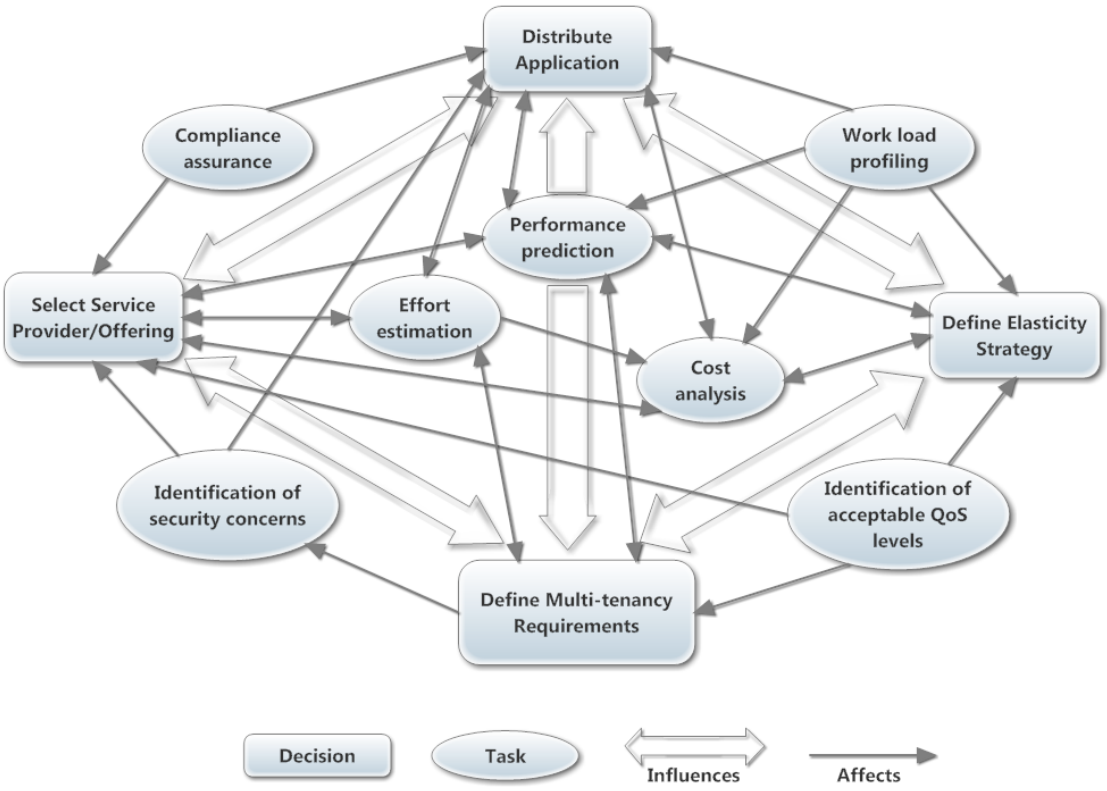
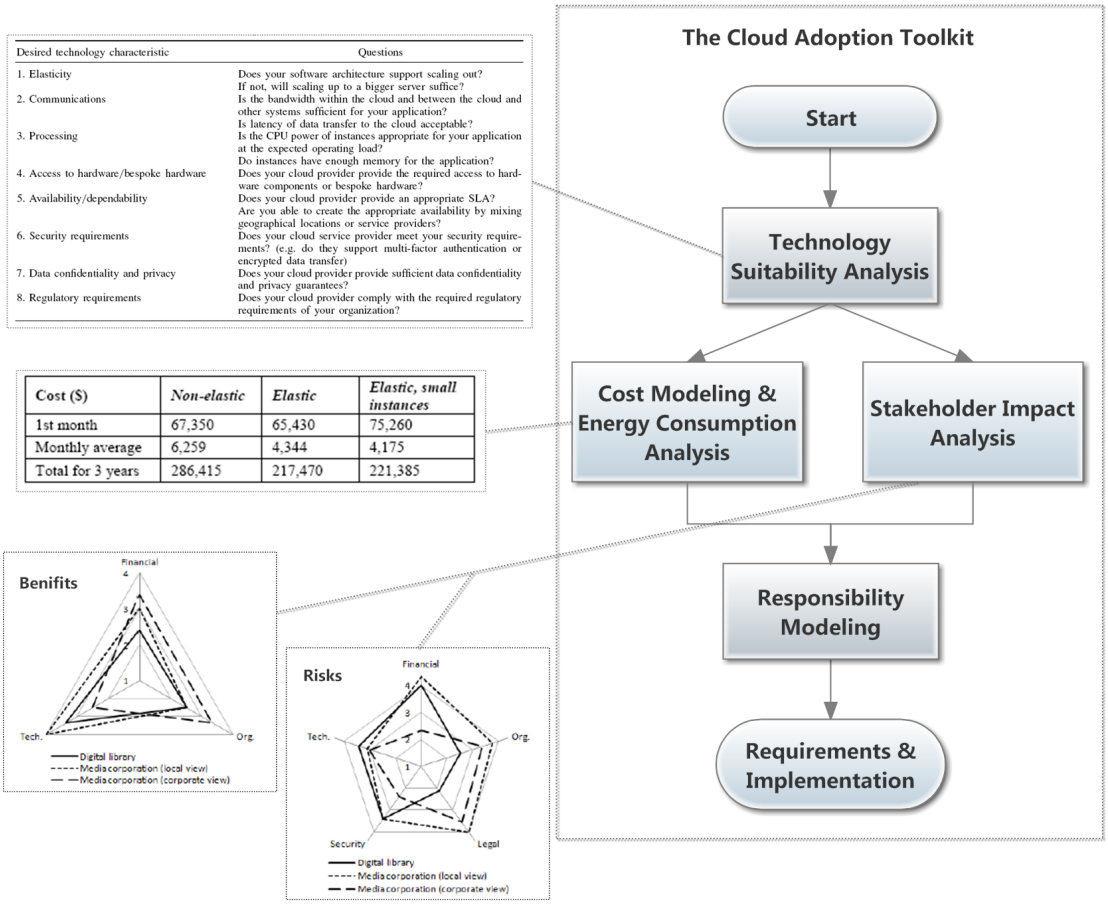


Figure 2.2: Conceptual Model of Decision Support System for Cloud Migration [9]

In comparison with the fore-mentioned decision support system, Khajeh-Hosseini et al. [8] developed a Cloud Adoption Toolkit to support decision making. This cloud Adoption Toolkit contains a conceptual framework and a mechanism to incorporate supporting tools, such as Technology Suitability Analysis, Energy Consumption Analysis, Cost Modeling, Stakeholder Impact Analysis and Responsibility Modeling.

The conceptual framework with toolkits for Cloud decision making is provided in Figure 2.3. Decision maker starts from the phase *Technology Suitability Analysis*, which aims to support in determining whether the Cloud technology is indeed needed or not. It refers to a checklist of 8 characteristics with 12 questions, as shown in Figure 2.3, to access the potent suitability of a particular Cloud service for a specific IT System. If the result of this analysis is positive, it can proceed to the further analysis. For the next step, decision maker may choose a *Cost Modeling* of running a server infrastructure on the Public Cloud, or an *Energy Consumption Analysis* of his own private Cloud infrastructure. The calculation of cost is based on UML deployment diagram which models a deployment of its own system on the Cloud. This model gives an accurate estimate of costs of the system with considering future resource demands. At the meanwhile, the *Stakeholder Impact Analysis* can be also implemented to help assessing the benefits and risks of a proposed IT system. The weighted values of benefits or risks classified in 5 categories are illustrated as radar diagrams, which are shown in Figure 2.3 as examples from the research by Khajeh-Hosseini et al. [7]. If all the analyses above indicate that the Cloud adoption is feasible, it comes to the next step: *Responsibility Modeling*, which is to

identify and analyze risks, and to check the operational viability of the complex IT system. And the last step is to complete the *Requirements & Implementation* of the system on the Cloud.



Desired technology characteristic	Questions
1. Elasticity	Does your software architecture support scaling out? If not, will scaling up to a bigger server suffice?
2. Communications	Is the bandwidth within the cloud and between the cloud and other systems sufficient for your application? Is latency of data transfer to the cloud acceptable?
3. Processing	Is the CPU power of instances appropriate for your application at the expected operating load? Do instances have enough memory for the application?
4. Access to hardware/bespoke hardware	Does your cloud provider provide the required access to hardware components or bespoke hardware?
5. Availability/dependability	Does your cloud provider provide an appropriate SLA? Are you able to create the appropriate availability by mixing geographical locations or service providers?
6. Security requirements	Does your cloud service provider meet your security requirements? (e.g. do they support multi-factor authentication or encrypted data transfer)
7. Data confidentiality and privacy	Does your cloud provider provide sufficient data confidentiality and privacy guarantees?
8. Regulatory requirements	Does your cloud provider comply with the required regulatory requirements of your organization?

Cost ($)	*Non-elastic*	*Elastic*	*Elastic, small instances*
1st month	67,350	65,430	75,260
Monthly average	6,259	4,344	4,175
Total for 3 years	286,415	217,470	221,385

Figure 2.3: Cloud Adoption Conceptual Framework [8]

2.3.2 Cloud Adoption Toolkit

In the Section 2.3.1 we have already introduced the Cloud Adoption Toolkit from Khajeh-Hosseini et al. [8], which consists of a conceptual framework for organizing decision makers concerns and a mechanism to incorporate supporting tools for each of these concerns. This toolkit aims to help the decision makers with assessing the feasibility of the adoption of cloud computing in their organizations and provides a collection of tools / techniques applied with a definite order: Technology Suitability Analysis, Energy Consumption Analysis, Cost Modeling, Stakeholder Impact Analysis and Responsibility Modeling. Among these, Stakeholder Impact Analysis is a most mature tool in the toolkit. The purpose of Stakeholder Impact Analysis is to support judging the socio-political feasibility or assessing the benefits and risks of a proposed IT system. The cloud adoption project is usually a complicated process of reconfiguration of working practices and technologies, accompanied with taking advantaging of expected benefits

and avoiding unexpected risks. Stakeholder Impact Analysis is just a method to identify the potential sources of benefits and risks from aspects of multiple stakeholders. This includes:

- Identify key stakeholders that could potentially affect or be affected by the proposed intervention
- Identify the changes in the tasks they would be required to perform and how they perform
- Identify the impact of these changes in terms of socio-political factors of the stakeholders
- Analyze and assess these changes in wider relational context
- Determine whether these changes are appropriate for stakeholders in the relational context or not

Certainly there are many factors which can influence the impact of the changes to stakeholders work activities, such as practicalities (time, resource and capabilities), social factors (value, status and satisfaction) and political factors (fairness of decision making procedure, distribution of benefits and risks).

By Stakeholder Impact Analysis a series of data are collected and processed with weights. In order to have a visualized understanding and a holistic picture of the benefits and risks from enterprises perspective, the weighted average of benefits or risks can be calculated and illustrated as a radar diagram, as shown in Figure 2.3. The benefits and risks can be identified in 5 categories (*financial*, *legal*, *organizational*, *technical* and *security*) and the weights of benefit/risk in the category are defined from 1 (unimportant) to 5 (very important). The weighted average can be calculated by multiplying the number of benefit/risk with different weights in each category and dividing the total number of benefit/risk in this category.

To identify the weight of the benefit/risk, a questionnaire or an interview is usually used among the stakeholders. By analyzing the data collected the benefits and risks of cloud migration can be summarized in tables, see Table 2.1 and Table 2.2 as examples. The second column in these two tables concerns the number of specific benefits/risks, which can help to decide the distribution of benefits/risks in different areas. As shown in the tables, 12 benefits as well as 18 risks are identified.

Benefits	#
Opportunity to manage income & outgoings	3
Opportunity to offer new products/services	2
Improved status	2
Removal of tedious work	2
Improve satisfaction of work	1
Opportunity to develop new skills	1
Opportunity for organizational growth	1

Table 2.1: Sources of benefit identified by Stakeholder Impact Analysis [8]

Risks	#
Deterioration of customer care & service quality	3
Increased dependence on external 3rd party	3
Decrease of satisfying work	3
Departmental downsizing	2
Uncertainty with new technology	2
Lack of supporting resources	1
Lack of understanding of the Cloud	1

Table 2.2: Sources of risk identified by Stakeholder Impact Analysis [8]

Furthermore, a Stakeholder Impact Analysis Matrix is used by some organizations [17]. This matrix contains more information in one table in contrast to the way defined by Khajeh-Hosseini et. al.. It enables stakeholder mapping and identification of key gaps, provides analysis of how stakeholders are involved, identifies stakeholder constituencies, gives insight into scale and extent of short term impacts, and even provides data for targeting and accounting for long term impact analysis.

A related work about risk identification and cloud adoption toolkit is published by Karim Djemame et. al. [18]. In this work they try to analyze and address the risk factor in cloud service system for optimizing service and design and implement an effective risk assessment framework, which contains methodologies of risk identification, evaluation, mitigation and monitoring, for cloud service provision. Among these, the way how they identify risk is for us most referential.

From their assumption, risk can be considered at all phases of interactions and investigated at each service stage in cloud computing. And there are two stakeholders

involved: Service Providers (SP) during service deployment and operation and Infrastructure Providers (IP) during admission control and internal operations. Additionally, risk can be assessed based on 4 categories: Technical, Policy, General and Legal. An example of risk category is presented in Figure 2.4. In each category, risk item will be assessed according to the level of impact and likelihood. The impact of risk ranges from 1 to 5 (1 - very low, 2 low, 3 medium, 4 high, 5 very high) as well as the likelihood to show its intensity. The risk level can be identified by the result of likelihood multiplying impact and therefore classified in a range from 1 to 25. Under the identification of the risk level the corresponding mitigation strategies will be chosen, which are listed in the risk inventory to determine how certain risks can be managed and evaluated to an acceptable level. Certainly risk assessment also depends on the time of operation during the cloud service lifecycle, which allows the risk level to change over time. With assessing various risk factors and identifying of associated mitigation solutions, appropriate mitigation strategies will be determined to optimize the execution of these mitigation solutions.

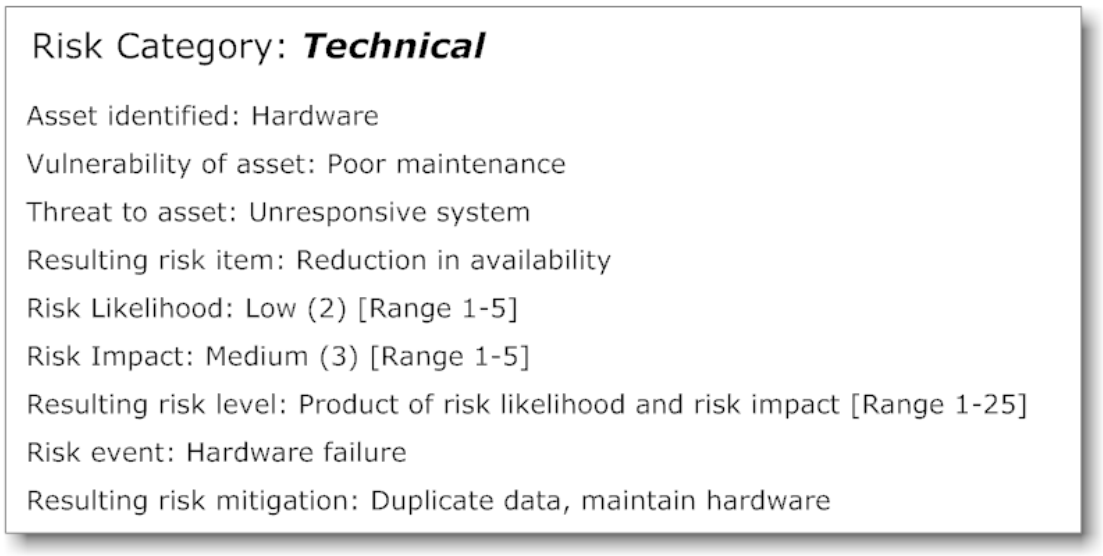


Figure 2.4: An example of risk category [18]

2.4 Risk Management

According to the ISO 31000 (2009) risk is defined as the effect of uncertainty on objectives, where uncertainties refers to the events, which may happen or not, and caused by lack of information. Risks can lead to a series of positive or negative consequences in terms of economic performance, professional reputation, safety, compliance, strategy, as well as environmental and societal outcomes. Thus, risk management is even more important to organizations or enterprises in modern society.

Risk management is a critical part of any strategic management. It involves identifying, analyzing, assessing and taking steps to reduce or eliminate the loss towards an organization or individual. The application of risk management utilizes many tools and techniques to manage various risks. At the meanwhile, several risk management standards have been developed by different organizations, such as the National Institute of Standards and Technology, the Project Management Institute and ISO standards as well.

ISO 31000, *Risk management Principles and guidelines*, is a standard of risk management codified by the International Organization for Standardization in 2009. It provides principles, framework and a process for managing risks and can be applied for any public, private or community enterprise, association, group or individual [19]. Therefore ISO 31000 is not intended to be specific to any industry or organization, rather to provide a common paradigm and guidelines to all activities concerned with risk management.

2.4.1 External and Internal Factors

The risks can result from factors both external and internal to the organization. The Figure 2.5 summarizes some specific risks and show in which areas they react. These risks can be divided here into four types [20]:

- Financial Risks, which include risks from:
  - price (e.g. asset value, interest rate, foreign exchange or commodity)
  - liquidity (e.g. cash flow, call risk, opportunity cost)
  - credit
  - inflation or purchasing power
  - hedging or bisis risk

- Strategic Risks, which include risks from:
  - reputational damage (e.g. trademark ro brand erosion, fraud, unfavorable publicity)
  - competition
  - customer demands

  - demographic and social trends
  - technological innovation in industry
  - capital availability
  - regulatory and political trends

- Operational Risks, which include risks from:
  - business operations (e.g. human resources, product development, capacity, efficiency, product/service failure, channel management, supply chain management, business cyclicality)
  - empowerment (e.g. leadership, change readiness)
  - reuglations
  - board composition
  - information tchnology (e.g. relevance, availability)
  - information or business reporting (e.g. budgeting and planning, accounting information, pension fund, investment evaluation, taxation)

- Hazard Risks, which include risks from:
  - natural or environmental damage
  - theft and other crime, personal injury
  - business interruption
  - disease and disability of employees
  - liability claims
  - contracts issues

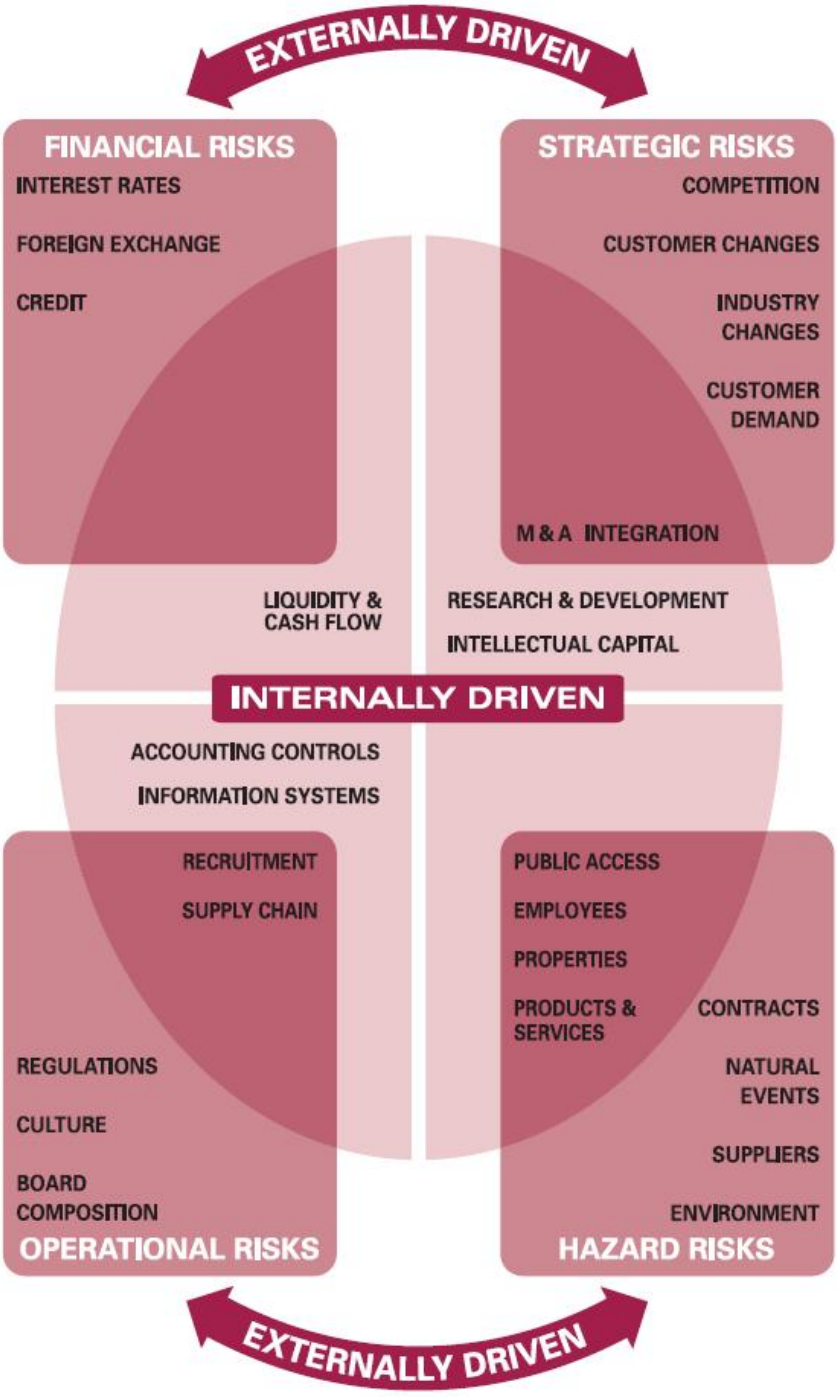


Figure 2.5: Drivers of Key Risks [6]

2.4.2 Risk Management Framework

Risk management framework consists of a set of components that provide the foundations and organizational arrangement for designing, implementing, monitoring, reviewing, and continually improving risk management processes throughout the organization [19]. It follows Plan-Do-Check-Act quality model, includes all key steps in the implementation and supports the risk management process. Figure 2.6 shows us a simplified version of the framework with details of implementation according to ISO 31000. However, ISO 31000 aims to provide a framework for implementing risk management, rather than a framework for supporting the risk management process.

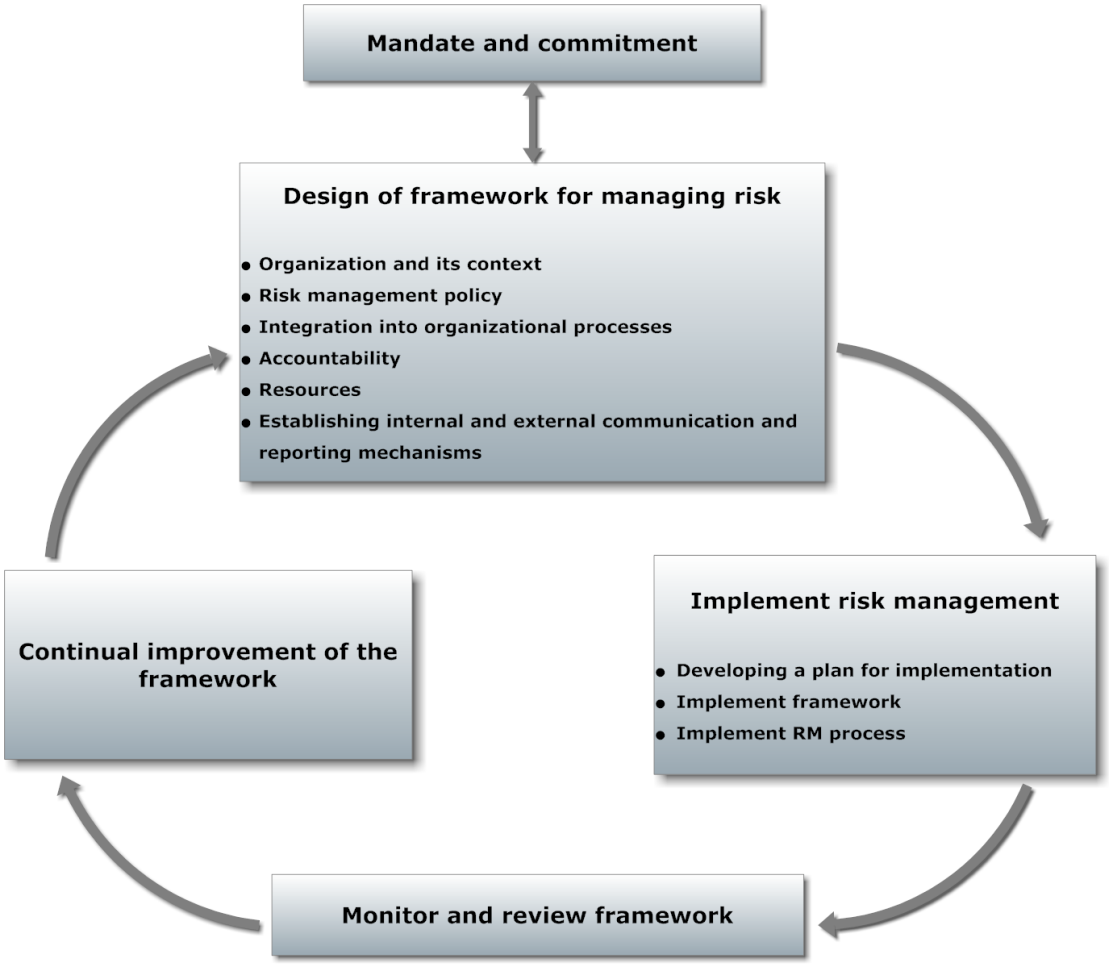


Figure 2.6: ISO 31000 Framework for risk management [19]

2.4.3 Risk Management Process

The risk management process is presented as a list of interacted, coordinated activities and events. Certainly there are many different descriptions of this process, but **7Rs** and **4Ts** of components labeled by IRM (Institute of Risk management) are usually included:

- Recognition or identification of risks
- Ranking or evaluation of risks
- Responding to significant risks
  - Tolerate
  - Treat
  - Transfer
  - Terminate
- Resourcing controls
- Reaction planning
- Reporting and monitoring risk performance
- Reviewing the risk management framework

According to the standard ISO 31000, the process of risk management consists of 6 steps as follows:

1. Establish the context
   - Establish the external context
   - Establish the internal context
   - Establish the risk management context
   - Develop risk criteria / threshold
   - Define the structure of risk analysis

2. Identify the risks
   - What can happen? How can it happen? Why could it happen?
   - Identify the retrospective risks
   - Identify the prospective risks
   - Refer to key processes, tasks, activities

3. Analyze the risks

- Identify the existing strategies and controls
- Determine the probability of the risk-occurrence
- Identify the Impact of the risk
- Estimate the level of the risk

4. Evaluate the risks
   - Identify the tolerable risks
   - Prioritise the risk for treatment
   - decide the acceptability of the risks

5. Treat the risks
   - Avoid the risk
   - Change the probability of risk-occurrence
   - Change the consequences
   - Share the risk
   - Retain the risk

6. Monitor and review
   - Review the effectiveness of treatment plan and the costs
   - Assess the final risk profile
   - Compare assessed alternative options

Throughout each step it is essential that there is consultation and communication with everyone in organizations functions, activities and events. See Figure 2.7

2.5 Summary

In this chapter the basic knowledge of cloud computing and its development status are firstly introduced. The definitions of deployment models as well as the classification of migration types are applied as foundation concerns of this work. Then we refer to the concept of decision support system by sharing several models and framework for cloud adoption, which is used to simplify the risk identification for the users in this work. At last, a general understanding of risk management according to ISO 31000 is given with its framework and process, which offer a hint of how to identify and assess the risks in cloud migration.

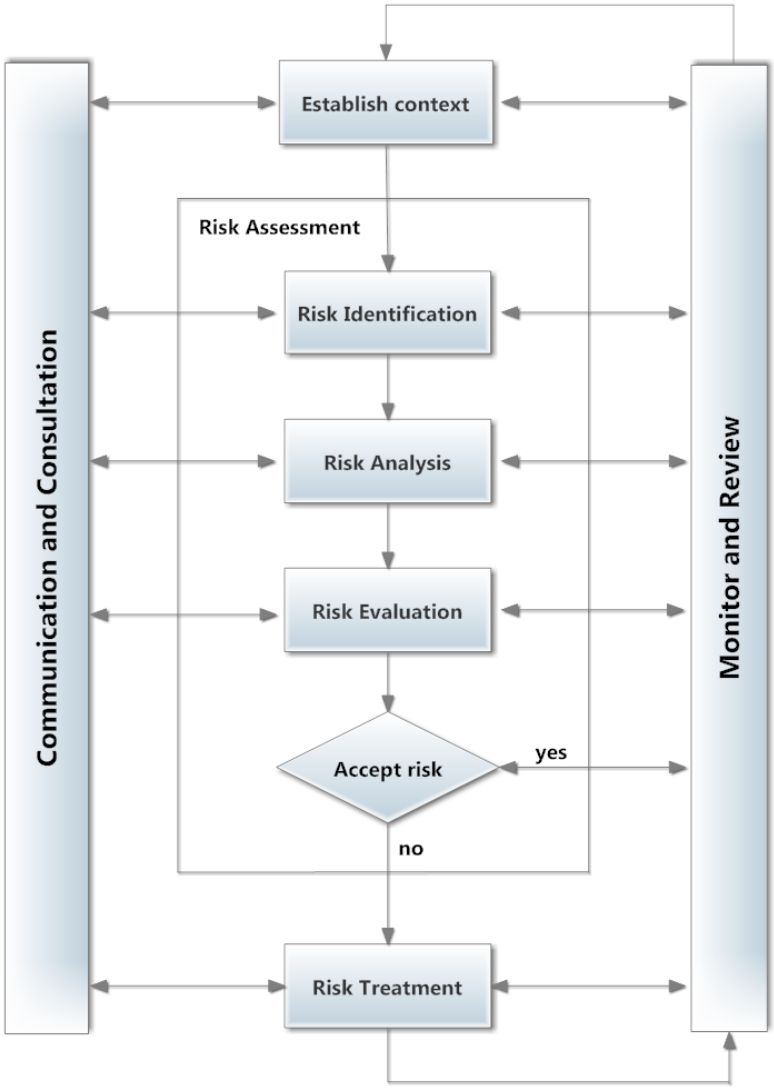


Figure 2.7: Risk Management Process [19]

3 Risk Assessment for Cloud Migration

3.1 Catalogue Creation Process

In this section we try to explain the process and the way of how the new catalogue of risk identification is created. Our risk catalogue is founded on the risk description standard defined by IRM and applies it to identify the risks of cloud migration by referring to a large number of academic papers and reports. The most heuristic reference of this catalogue is the method of identifying risks and the spreadsheet (available from PlanForCloud.com) by Khajeh-Hosseini et al. [5].

3.1.1 Risk Description Standard

According to the definition by IRM, identified risks can be displayed in a structured format - risk description table, as presented in Table 3.1. This table can be used to facilitate the description and assessment of risks. A well designed risk description structure should contain sufficient informations about the risks name, reference, how it could happen, stakeholders and their expectations, probability of its occurrence, influence and consequence when it happens, and some treatments or improvement should also be involved in order to eliminate risks or mitigate the impacts. With all these informations a relative comprehensive understanding about risks would be obtained, which could happen in the whole business process. This work is based on the general risk description standard from IRM and has applied it into the risk identification and assessment in cloud migration.

1. Name of Risk	
2. Scope of Risk	Qualitative description of the events, their size, type, number and dependencies
3. Nature of Risk	Eg. strategic, operational, financial, knowledge or compliance
4. Stakeholders	Stakeholders and their expectations
5. Quantification of Risk	Significance and Probability
6. Risk Tolerance/ Appetite	Loss potential and financial impact of risk Value at risk Probability and size of potential losses/gains Objective(s) for control of the risk and desired level of performance
7. Risk Treatment & Control Mechanisms	Primary means by which the risk is currently managed Levels of confidence in existing control Identification of protocols for monitoring and review
8. Potential Action for Improvement	Recommendations to reduce risk
9. Strategy and Policy Developments	Identification of function responsible for developing strategy and policy

Table 3.1: Risk Description by IRM [6]

3.1.2 Process of Risk Identification

To create the new catalogue of risk identification involves 4 steps, which is illustrated in Figure 3.1:

1. Make a clear understanding of the spreadsheet of risk identification by Khajeh-Hosseini et al. and analyze each risk description to verify whether it happens indeed by cloud migration or discuss whether it can be merged with other risks.
2. Add risks which are not included in this spreadsheet by referring to other related works.
3. Collect and reclassify all the risks with 5 new categories (Compliance, Financial, Knowledge Management, Operational and Strategic).
4. Adapt all these risks into IRM template with adding all information needed.

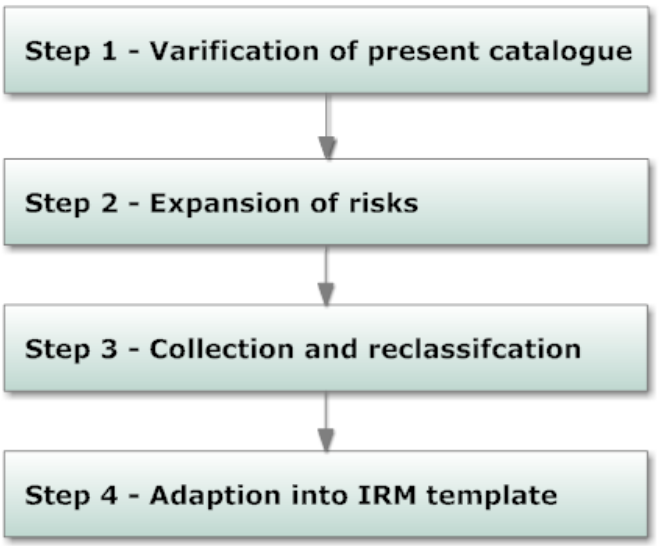


Figure 3.1: 4 Steps of Risk Identification

First of all, the risk identification by Khajeh-Hosseini is used as a foundation of our new risk catalogue. This risk catalogue is available from PlanForCloud.com as a Google Docs spreadsheet. This spreadsheet has two tabs, one for benefits and one for risks, which aims to support risk management and ensure that the decision makers can make informed trade-offs between the benefits and risks of using the cloud. In comparison with the 5 categories in risk type (Compliance, Financial, Knowledge Management, Operational and Strategic) defined by IRM, 39 risks are classified also in 5 categories (Organizational, Legal, Security, Technical and Financial) with their descriptions and mitigation approaches in this spreadsheet. After a thorough analysis of this work most of the exiting risks are remained since they are proved in many literatures to be occurring during cloud migration. For example, R1 defines a situation, in which the users can purchase computing resources using their own credit cards without explicit approval from

central IT department. This may cause loss of governance or control over resources in both physical and managerial aspects, which is also described in many other documents such as the work from J. Dibbern [21]. We maintain this risk with a proper name in our catalogue and classify it later into the type *Strategic*. Some risks like R38, which describes uncontrollable sources of data transfer delay or bottlenecks, are omitted due to lacks of reference in other documents. However there are also some risks that can be emerged to other risk. For example R8 explains a similar context of risk of loss of governance and control over systems like R1, only in the aspect of service quality. So we arrange these two risks with one ID in the new catalogue.

After rearrangement of present spreadsheet, some risks should be also taken into account in the risk collection in step 2. For example, there are many articles and reports mention that nature disaster could be a threat for cloud computing. Hurricanes, earthquakes or fires may destroy the hardware or database of cloud provider and the user's data could be damaged or lost, as described in such report by ENISA [3]. But there is no corresponding description in Khajeh-Hosseini's spreadsheet. Therefore we add this into the new risk catalogue as well.

In step 3, we collect all the risks found and reclassify them with new categories defined by IRM risk standard. According to the Khajeh-Hosseini's spreadsheet, risks are classified in 5 categories with organizational, legal, technical, security and financial. After analysis we learned that the risks in *Financial* refer to ineffective management and control of the costs of an organization and other threats in financial issues such as credit, foreign exchange rates etc.. These risks that are in the original category financial should be maintained with the same categorys name, such as R34 in the spreadsheet, which is identified with R8 "over budge" in the new catalogue. However some risks should be separately relegated, because these could happen in phase of planning when the management team made an inappropriate decision on cloud migration. Differing from other organizational risks, these risks can lead a series of negative consequences with enormous loss. Therefore a new category in strategic is on demand and certain risk such as R1 by Khajeh-Hosseini is corresponding to R39 with *Strategic* in our catalogue. Similarly there are some risks that the organization is everyday confronted in order to achieving the strategic goal. These should also be categorized into a new type named *Operational* from those organizational risks, e.g. the former R11 in organizational, which describe a situation in resistance to change resulting from organizational politics and changes of working manner, is now identified with R32 in *Operational*.

After collecting all the risks that are from the original organizational from spreadsheet into strategic and operational, we found that some legal risks such as R16 from the spreadsheet, which is non-compliance with data confidentiality regulations, should be re-categorized in *Compliance* according to IRM standard. Besides, those risks of security in former catalogue describe certain scenarios in which data may be threatened due to technical problems such as browser vulnerabilities in R25 or interception of API messages in transit in R23. Since *Knowledge Management* by IRM is defined to concern all the knowledge and technical issues, we categorize the risks of security into this type. Certainly all the technical risk like R28, which is about the bad service performance, should also be categorized in *Knowledge Management*, since it refers to ineffective management and control of the knowledge resources and technologies.

After all 3 steps, a new list of risks of using cloud is available. We have to adapt them into IRM standard of risk description, which is explained in Section 3.1.1. This IRM template defines 9 attributes for each risk while Khajeh-Hosseini has identified only 4 main features. By referring a plenty of literatures we supply all the lacking information into corresponding item of this template and name each risk briefly and clearly in step 4.

Finally we have a new catalogue with 46 risks by cloud migration, which include all information according to IRM standard of risk description. In this new catalogue 37 risks from original spreadsheet are maintained and modified in 34 risks by merging and separating risks. 12 new risks are created, which are listed in Table 3.2 with their ID, name and new category of nature. More information of the new risks is available in Appendix A.2

ID	Risk Name	Risk Nature
R1	natural disaster	Compliance
R7	subpoena and e-discovery	Compliance
R11	inablity to recuce costs of hardware	Financial
R16	physical failures	Knowledge Management
R27	social engineering attacks	Knowledge Management
R30	loss of backups of user	Knowledge Management
R35	supply chain failure	Operational
R38	lack of standards	Operational
R40	change of cloud service	Strategic
R41	poor provider selection	Strategic
R43	log & tracing failure	Knowledge Management
R45	VM breakdown	Knowledge Management

Table 3.2: New Risks in Comparison with Spreadsheet from PlanForCloud.com

3.2 Risk Catalogue (Cloud Migration)

In the new catalogue, 46 risks in all are identified with 9 attributes and features for each risk. In following section we try to discuss these attributes by explaining which information is corresponding to which attribute. The whole catalogue is available in Appendix A.2.

3.2.1 Name of Risk

In the table of risk description by cloud migration, we try to name the risk with some brief and clear phrases, such as over budget or service disruption, in order to describe the risk simply but accurately when referring this risk. For example, R9 describes the scenario, in which the actual costs may be more than expected caused by inaccurate resource estimates or service prices changing by cloud provider. We simplify this situation with "over budget" and summarize the descriptions into "Scope of Risk". Combining with the *Scope of Risk* in Section 3.2.2, a general understanding of this risk can be got.

3.2.2 Scope of Risk

The scope of risk here refers to the qualitative description of the events, and possibly with their size, type, number and dependencies. In this work we try to describe detailed the circumstance or the condition, in which risk may occur by the migration into the cloud, as for example R9 shown in Section 3.2.1

3.2.3 Nature of Risk

According to the standard by IRM, business activities and decisions can be classified in 5 categories [6]:

- Compliance
  This refers to the issues such as health & safety, environment, trade descriptions, consumer protection, data protection, employment practices and regulatory issues.
- Financial
  This refers to the effective management and control of the costs of an organization, and other financial issues such as credit, foreign exchange rates, interest rate movement and other market exposures.
- Knowledge management
  This refers to effective management and control of the knowledge resources, technologies, the production, protection and communication. This also concerns some external factors such as user authentication and intellectual property protection, even area power failures and technical competitiveness. System breakdown and loss of key staff etc. could be involved as internal factors of knowledge management as well.

- Operational
  This refers to the issues, which the organization is everyday confronted in order to achieving the strategic goal, such as resistance from the stuff or reduction of productivity due to new manner of working, or supply chain breaking.
- Strategic
  This concerns to the long-term strategic objectives of the organization. This refers to capital availability, legal and political issues, and reputation and changes in the physical environment.

In this work we also identify the nature of the risk in 5 categories which is based on the IRM standard, i.e. 5 risks from the new catalogue are in strategic, 6 in operational, 22 in knowledge management, 4 in financial and 9 in compliance. More information is available in Appendix A.2

3.2.4 Stakeholders

The stakeholders concern all the groups which can affect or be affected by the business activities, here specially the risks. The stakeholders can be either direct or indirect. Direct stakeholder may involve those people who can directly impact the risk or be impacted when risk happens. However indirect stakeholders are those who have political power to influence the occurrence of the risk or those who are interested in its outcomes.

In business activities the stakeholders may usually concern such as government, employees, clients, suppliers or community etc.. Considering of the risk aspect they may concern such as strategic team, legal team, budget department from the client side, or IT technology and security team from the side of service provider. In some cases they may refer to the government or the legal institutions as well.

In this work we refer the stakeholders of risk simply to *Cloud Client* (CC)and *Service Provider* (SP).

3.2.5 Quantification of Risk

Risk quantification refers to evaluating risks and risk interactions to assess the possibility of the occurrence of the risk. Table 3.3 could give sufficient thoughts and be unanimously recognized by all stakeholders before being used.

3.2.6 Risk Tolerance / Appetite

Risk Appetite and Risk Tolerance have usually deep associations with the financial services industry. In this work they are referring to the potential and financial impact on the organization due to the risk by cloud migration, and the probability and size of potential losses or gains. They also concern the objective for control of the risk and the

Score	Level	Description	Indicators
5	Very likely	This risk event is highly likely to occur with more than 90% probability	Could occur several times in a year or has occurred recently
4	Likely	This risk event is more likely to occur with the probability of 50% to 90%	Could occur yearly
3	Possible	This risk event may be occur with the probability of 30% to 50%	Could occur more than once within a period of 10 years
2	Unlikely	This risk event is not likely to occur with the probability of 5% to 30%	Could difficult to occur within a period of 10 years
1	Very unlikely	This risk event is hardly to occur with less than 5% probability	Has not occurred within a period of 10 years

Table 3.3: Probability of Occurrence - Risks [6]

desired level of the system performance. Table 3.4 classifies the impact of the risk in 3 levels, associated with description of each level.

3.2.7 Risk Treatment & Control Mechanisms

Risk treatment is the process of selecting and implementing of measures to modify risks [6]. It involves identifying the range of options for treating risk, assessing the options, preparing risk treatment and implementing. These options usually refer to [22]:

- Retain or accept the risk. The risk is considered as acceptable to the organization and being retained after controls.
- Reduce the probability of the risk occurring - by means of preventative maintenance, audit compliance programs, supervision, contract conditions, policies & procedures, testing, investment & portfolio management, training of staff, technical controls and quality assurance programs etc.
- Reduce the impact of the risk occurring by means of contingency planning, contract conditions, disaster recovery & business continuity plans, off-site back-up, public relations, emergency procedures and staff training etc.
- Transfer the risk this concerns the third party to bear or share the risk using contracts, outsourcing, insurance or partnerships etc.
- Avoid the risk decide to avoid the activities which can generate this risk.

Score	Level	Description
3	High	Significant impact on the organization's strategy or operational activities Significant stakeholder concern
2	Medium	Moderate impact on organization's strategy or operational activities Moderate stakeholder concern
1	Low	Low impact on organization's strategy or operational activities Low stakeholder concern

Table 3.4: Impact of Occurrence - Risks [6]

In the table of risk description A.2 we try to summarize the primary means by which the risk is currently managed according to all above mentioned methods and address them to the corresponding risk briefly but accurately. E.g. R1 with the mitigation method of "data duplicated for a backup on other location", or R12 with "use cloud middleware".

3.2.8 Potential Action for Improvement

In this column a number of proposals and recommendations are given to eliminate risk or mitigate the impact of the risks. Some of them can be achieved at present, such as R23 with "a duplicated system on another cloud is standby", and some may be done in the future, such as R8 with "establish global regulatory agreement with full transparency". It is difficult to give a practical mitigation of the risk such as natural disaster, and some improvements against risk are also beyond our knowledge, so we save it blank for the further work.

3.2.9 Strategy and Policy Developments

Achieve goals on policy is depending on having a clear strategic focus, objectives that are totally analyzed and researched, and delivery that is properly planned and managed. It rarely happens by chance. In this column the ID numbers of functions are provided, which are responsible for developing strategy and policy, in order to reduce the likelihood of the occurrence of the risks and even avoid risks. All the functions are listed with ID number and descriptions in Appendix A.1

3.3 Discussion & Summary

In this chapter we try to build up a risk catalogue in cloud migration by means of applying the risk description standard from IRM, using the exiting risk catalogue by Khajeh-Hosseini as basis and expanding the risk identification through plenty of references. 46 risks are identified in the new catalogue in comparison with 39 risks in the Khajeh-Hosseinis spreadsheet. Most risks are maintained and reclassified in 5 new categories. In the meanwhile some risks are omitted or merged by other risks in our catalogue. More information is added into the catalogue in order to adapt IRM template. This new catalogue is applied in the database of a decision support system, which will be introduced in next chapters.

4 Design & Implementation

This chapter focuses on the introducing requirements, presenting the specification and design, and explaining the implementation of a decision support system for Cloud migration. This migration support system aims to model and incorporate the identified risks and mitigation methods in guiding the user through the different types of migration to the Cloud, with an emphasis on the extensibility of the system. This system is based on RESTful services and implemented in Java language.

4.1 Requirements

Nowadays Cloud Computing is getting a big popularity in IT solutions, which offer a pay-as-you-use service with advantage of efficiency, flexibility and scalability. Certainly many risks may also happen within the process of migrating to the cloud. In the Section 2.3.2 we have already introduced some methods for risk identification, such as Stakeholder Impact Analysis by Khajeh-Hosseini et al., and risk category by Karim Djemame et.al.. Besides a risk spreadsheet from PlanForCloud.com is also explained in Section 3.1, which is used to discuss risks from different stakeholder perspectives in an arranged meeting. Furthermore we have also described all possible risks with their context of occurrence as well as the likelihood and consequences in a fine detailed IRM template. But for the user, who is planning to take advantage of the cloud services, there are no direct ways or such a visualized tool concerning the risks that may be confronted to help making decisions whether it is suitable for the migration and how to avoid or mitigate these risks. And with different cloud deployment models and migration types is the migration of components associated with different types of risks, which lead to decision making even more complicated. Therefore an easy using and efficient decision support system for risk assessment is on demand.

For our assumption, a comprehensive database of risks with information related is as the basis of this system. This database should contain all the risks that may be confronted in cloud migration and as much descriptions of each risk as possible, which describe the attributes and features of these risks. Then a friendly user interface with full functionalities should be provided in the system, which offers a concrete and direct interaction for the decision makers. In this UI an easy way of collecting users information is needed: using choices and making ticks instead of entering texts. After all requirements are collected, the system should search for all the associated risks and present them according to the risk types. All the risks should be listed with information, which are needed for the risk assessment. With these informations the user can get a general impression about how many risks would occur, and a concrete understanding about which risks in

which aspects he may confront, and how to mitigate the impacts of the risks or totally avoid. This will help the user for the future work in decision making. Besides, this system should also be platform independent in order to getting a better scalability and extensibility.

4.2 Specifications

According to the requirements all the users information should be logically collected in the user interface. Choosing the deployment model of Cloud whether an application is being migrated to a public cloud or private, or maybe hybrid, is firstly asked for. In order to get a clear understanding of the deployment models, some helping texts or hints could be offered optional. Then a migration type will be asked for choosing, which we have already discussed in the Section 2.2. For the sake of users some hints about the migration types could be provided with expandable buttons as well because the user may have an unclear understanding about the classification of migration type i.e. if they want to migrate only some components in one layer to the cloud they dont know how to choose the corresponding migration type. Besides, a number of questions will be asked to identify risks more accurately. After all requirements are collected, the system should search for all the associated risks and present them according to different risk types. All the main information about each risk should be listed in order such as risk name, type, context of its occurrence, and the mitigation methods as well. With all these informations the user could have a comprehensive understanding about the property of all possible risks and how to avoid or mitigate their consequence.

Based on the major features demanded and the existing methods for decision making that we have already introduced in former section, following details should be considered:

- Function
  The main function of this system is to collect the user requirements before cloud migration and return all the associated risks that may occur in the process of migration with detailed information. This system offers a comprehensive understanding of the risks confronted and their corresponding mitigation methods and enables helping the user for decision making. All the functions would be implemented as RESTful Web Services and the interface as a Web application.

- Interaction
  The system provides a pleasant, simple, user-friendly interface. The user interface acts as the Frontend of the system and a database as Backend. The interaction is realized between the user and the system where a set of requirements will be given by user and a listing of risks with detailed information as a system result.

- Data
  A risk database should be created, which contains all kinds of information about risks as well as the relationships between risks and deployment models, between

risks and migration types, and between risks and all associated questions. Furthermore all the questions as well as the hint information for selecting deployment models and migration type should also be involved in the database.

- System
  The system should be designed as program-language-independent as well as platform-independent for a better extensibility and scalability. And all the services can be put in a WAR file and able to run in other enviroments.

4.3 Design

4.3.1 System Overview

Figure 4.1 gives an overview of the conceptual architecture of the proposed migration decision support system, which is divided in to 2 parts: a user interface acts as Frontend and a risk database as Backend. Interaction will be implemented between UI and database by using RESFful Service. Entering user requirements includes 3 steps: first, once a deployment model for the migrating has been chosen, a series of corresponding risks will be identified. Second step, choosing the migration type will continue to narrow the search field. At last, a list of questions will be asked to ensure the specific risks, especially in some non-technical aspects. After all the requirements are collected, a comparison between user's requirements and risks in database will be achieved by RESTful service. And the result of RESTful service, which is seen as the result of searching, will be sent back to the user on the UI.

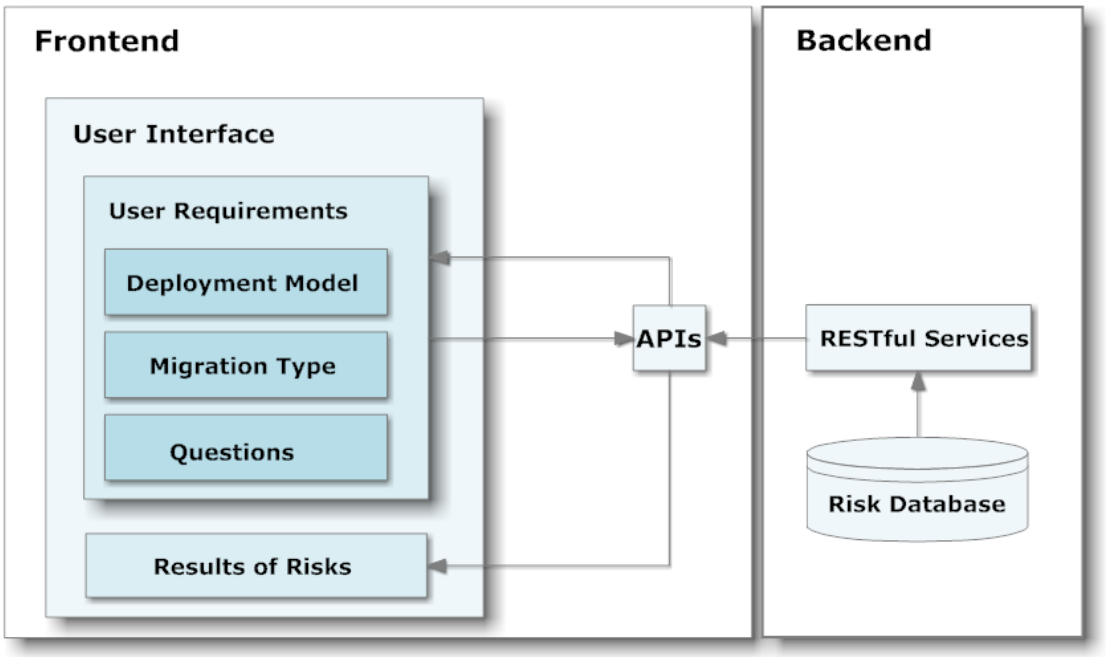


Figure 4.1: Architecture of System

4.3.2 Database

A risk database is the critical part of this system. In each step of decision support process this database is addressed for offering data and informations. Therefore this database should contain all the risk concerns as well as the relationships between entities.

According to the requirement analysis an Entity-Relation diagram is designed to implement the risk database of the system. This ER-diagram consists mainly of 4 Entities with their attributes and relationships among them, which is presented in Figure 4.2.The entity *Risk* is as the basic element in the ER-diagram, which all the other entities are related to it. There are 4 deployment models and each model can identify many risks which build these two entities a many-to-many relationship. Similar with the *Deployment Model*, the *Migration Type* has also a many-to-many relationship with *Risk*, since each type is corresponding to many risks. The entity *Questions* is supposed to have a one-to-many relationship with Risk because certain question can identify many questions.

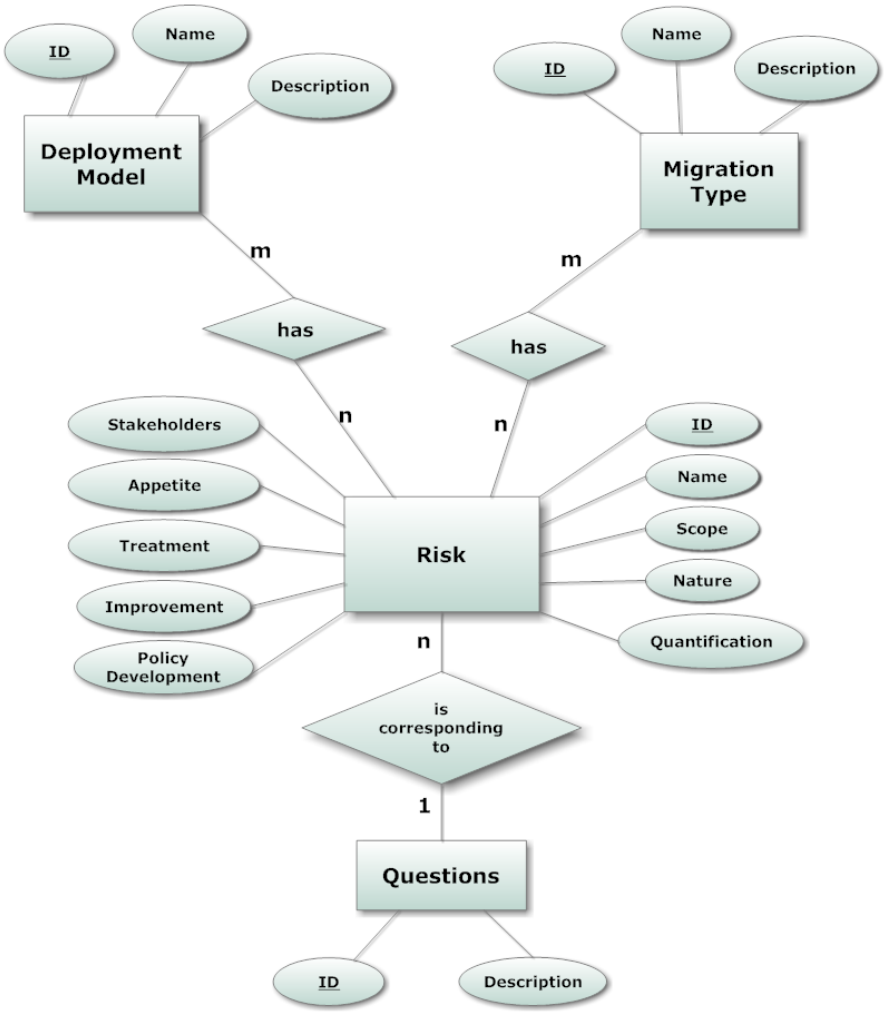


Figure 4.2: ER-Diagram of Risk Database

4.3.3 User Interface

In this section, the user interfaces of this decision support system are introduced with different scenarios. Balsamiq Mockups is used to set up these UIs, which are presented in following figures. Each UI consists generally of text fields, scroll bars and buttons. Text fields are applied to describe all the requirements as well as the hint information and scroll bar is used to simplify the interface. There are two types of buttons in use, ratio buttons are used to identify the users unique choice while normal button submit the instruction and ask for an execution.

The main page is in Figure 4.3 presented which acts as a dialogue window. It is divided into 2 parts: some system information and a salutatory are located in upper part, and in the lower part the users requirements are collected with some hint information shown optional. A scroll bar is on the right side in order to show other information and a main button for submitting the search order is at the bottom.

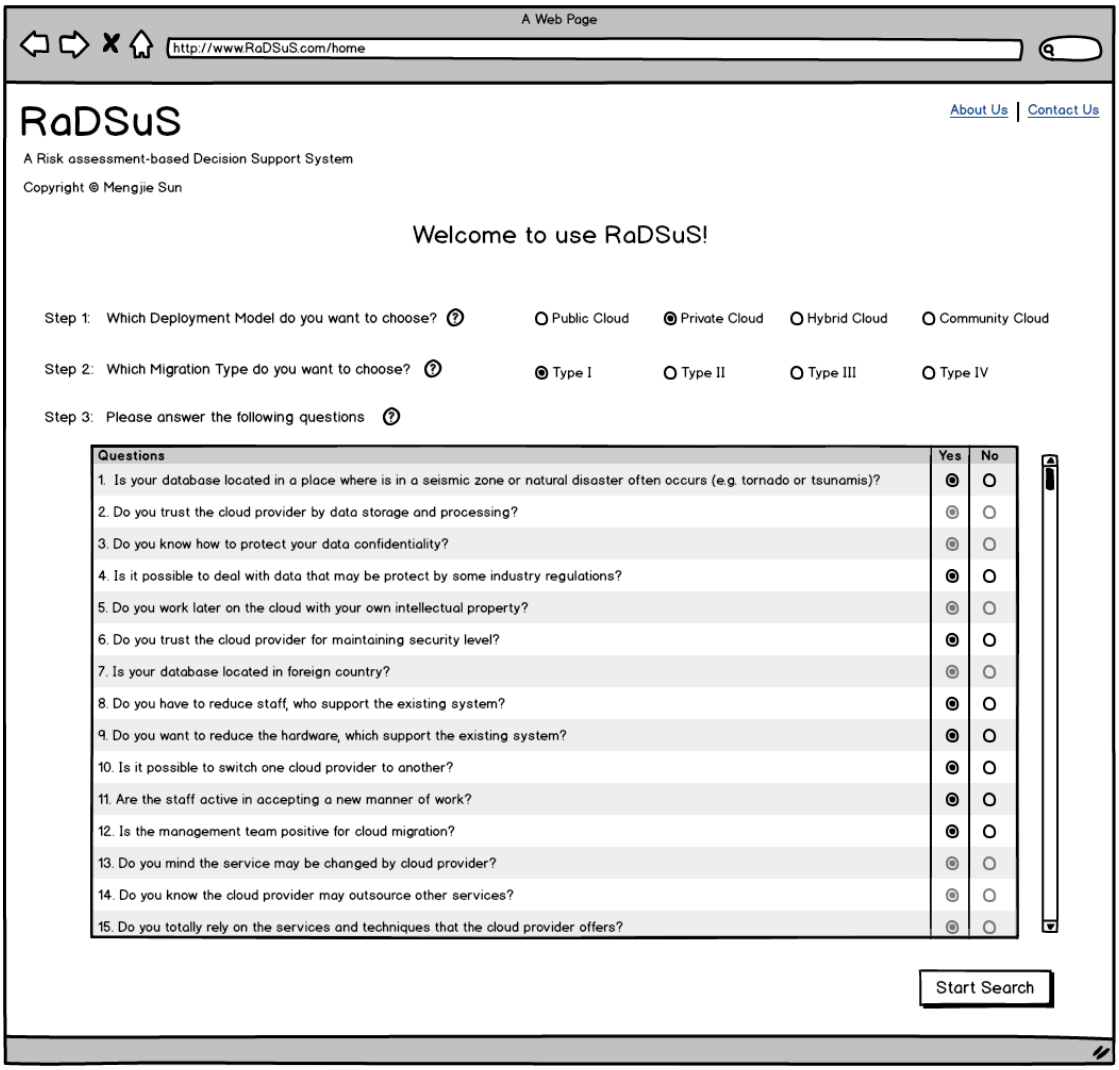


Figure 4.3: Homepage of RaDSuS

As demonstrated in Figure 4.3, 3 steps are set up to collect users requirements. Step 1 is asked for choosing a deployment model and the default choice is public cloud. There is a help button available beside step 1 question, which can activate a drop-down text field of hints, as shown in Figure 4.4. This aims to help the user for a better understanding of the definition of deployment models and making an appropriate determine.

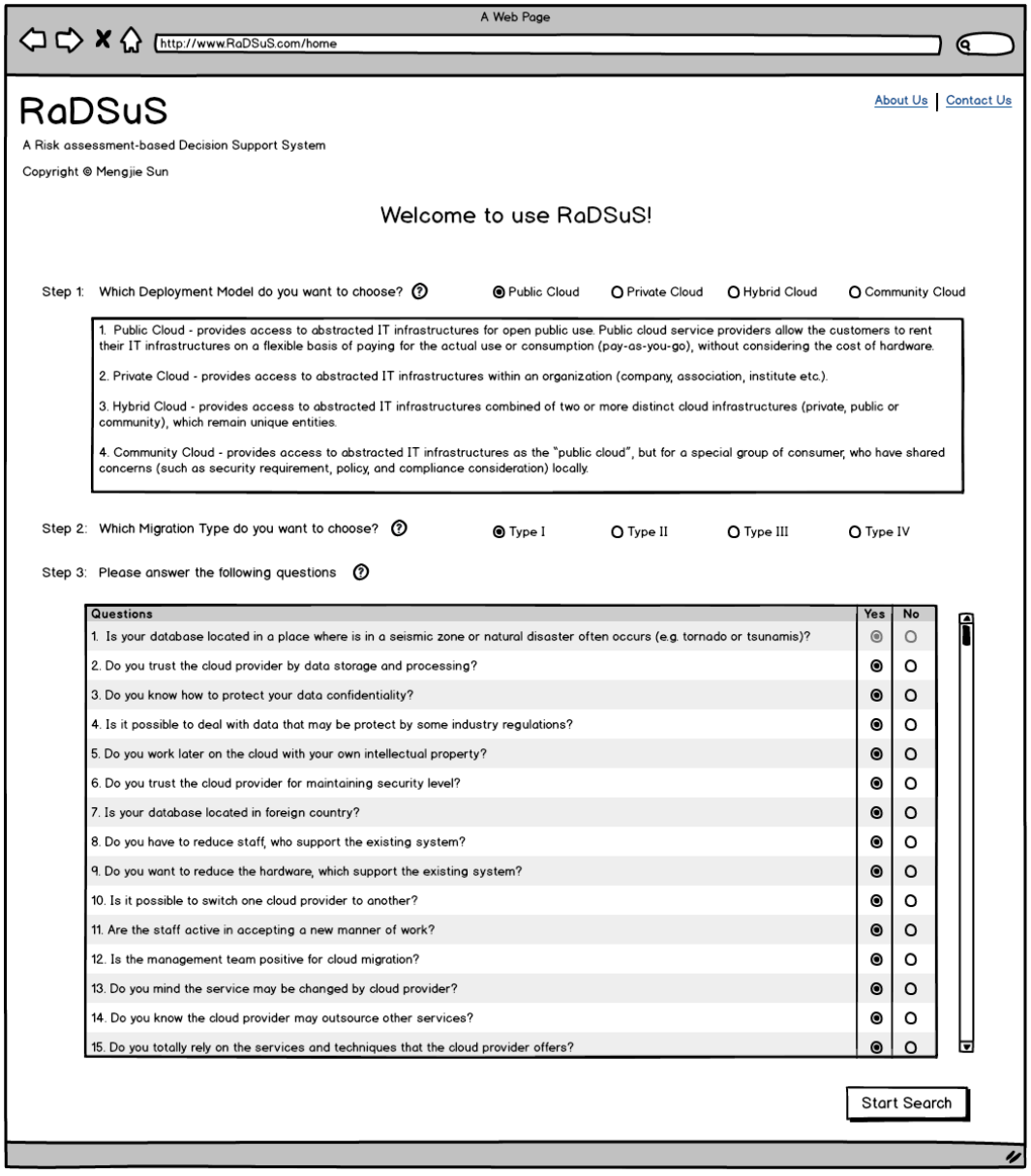


Figure 4.4: Hints of Deployment Models

Step 2 is about choosing the migration type. In the section 2.2.1 we have already explained how to classify the migration in four types. However the concepts of migration type may be unfamiliar to the user and a corresponding hint is on demand, which is shown in Figure 4.5. The default setting of migration type is Type I.

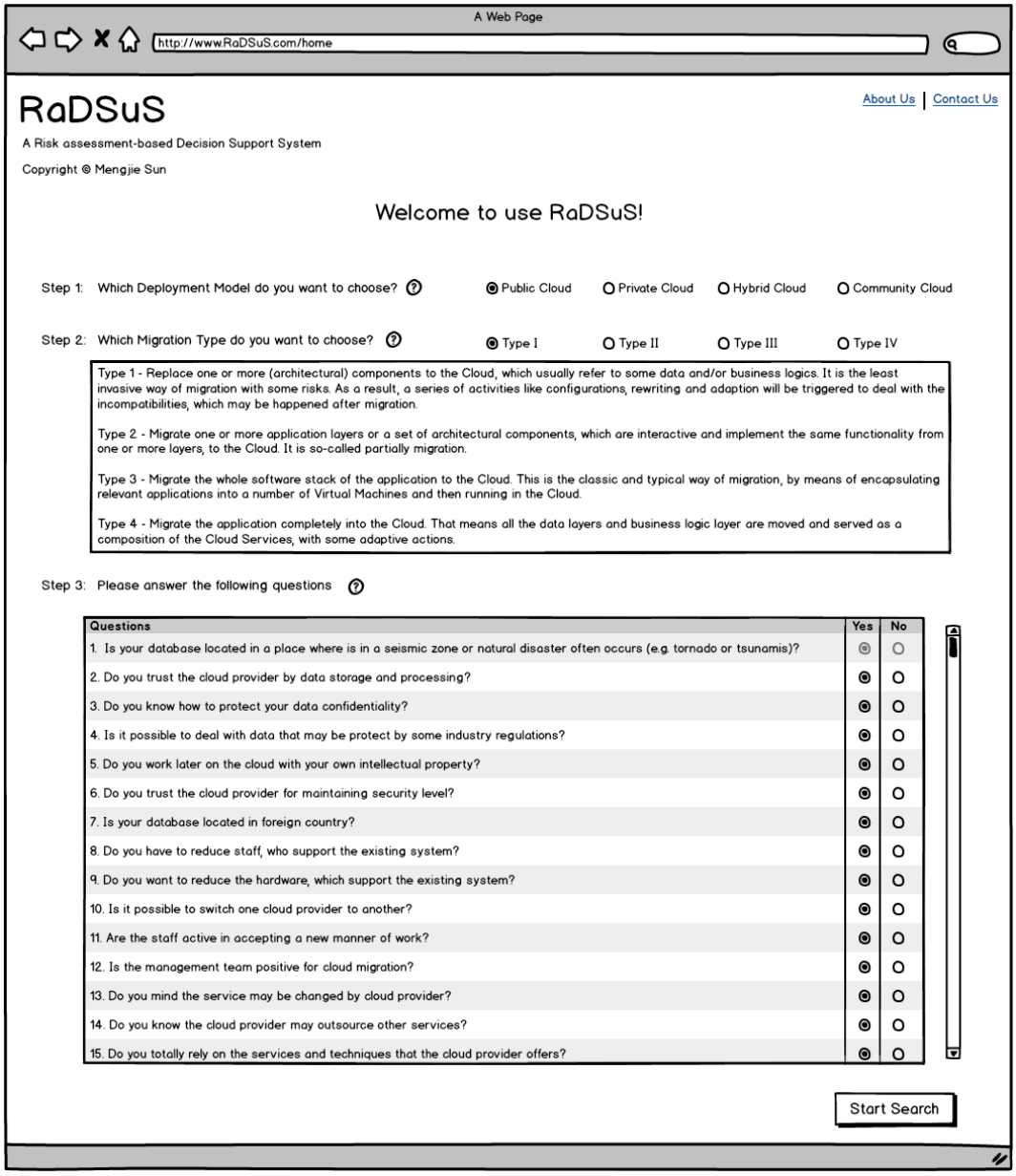


Figure 4.5: Hints of Migration Types

In step 3, a series of questions are asked for aiming to specify the requirements for a better searching ability of risks. These questions are for the IT experts and developers with concerning knowledge, as shown in Figure 4.6. There are also some explanations before answering these questions by clicking the button with question mark, about which are for those normal user who has no ideas. With a definite window of this UI, a scroll bar is needed here to maintain the concision of the interface. Each question will be answered with a ration box as same as the former two steps to keep the choice unique. The default answer of each question is yes if the user leaves the question with no answer, the system will return all the possible risks.

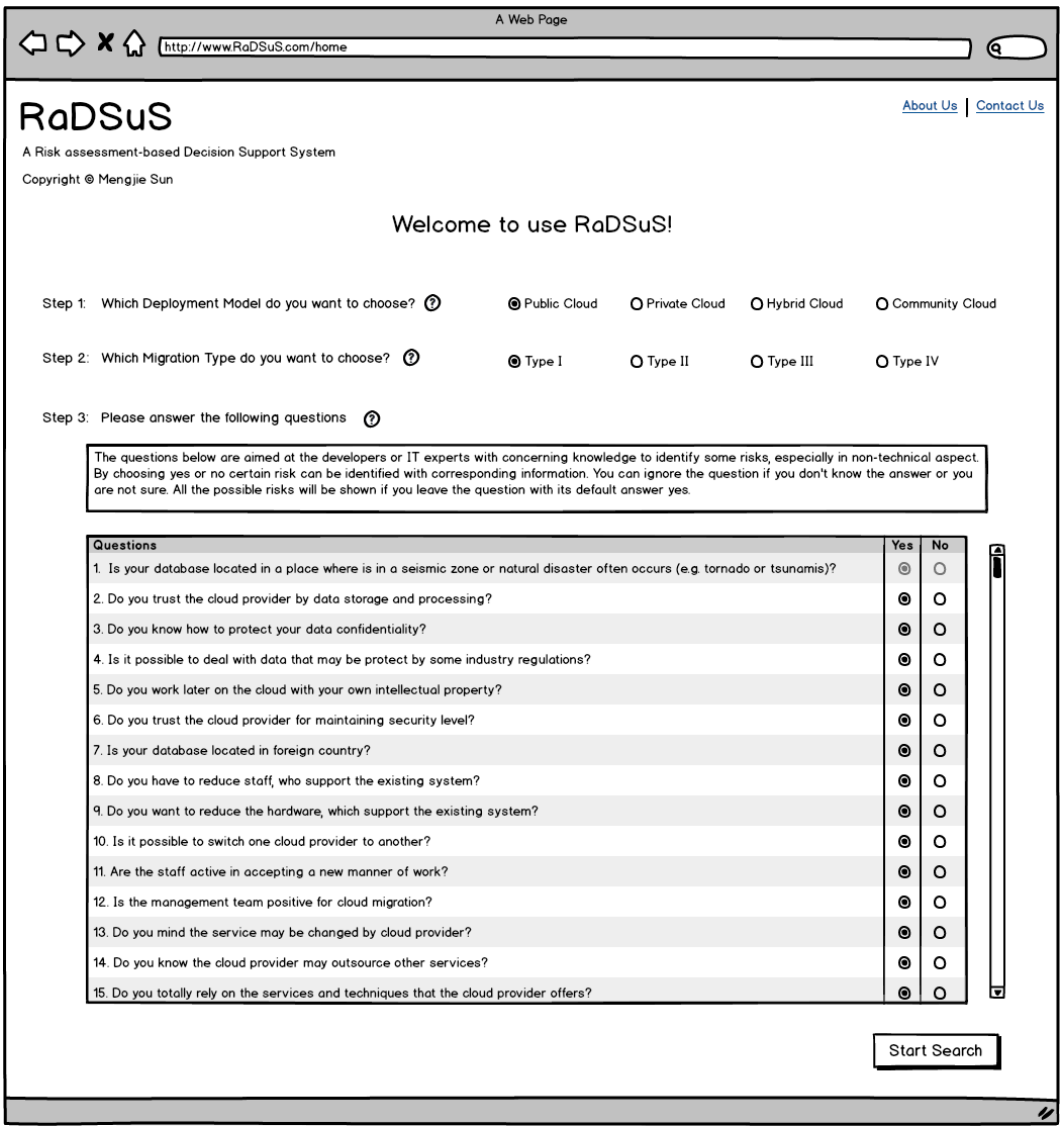


Figure 4.6: Hints before Answering the Questions

There are some constraints applied here in step 3. When the user has chosen private cloud in step 1, some questions are fading out due to the constraints in the database. This facilitates the questionnaire step for avoiding the user to answer the question which is related to identifying those risks that has been already removed from the result in the first step. Figure 4.7 demonstrates exactly this scenario. The first question "Is your database located in a place where is in a seismic zone or natural disaster often occurs (e.g. tornado or tsunamis)?" is default to be disabled because the default setting in step 1 is public cloud and this corresponding risk is exclusive from the search field of public cloud. We believe that this risk rarely happens by public cloud because the public cloud provider usually has a set of mechanisms to avoid its occurrence or an alternate backup data center. This will be presented in the main page of the system shown in Figure 4.3.

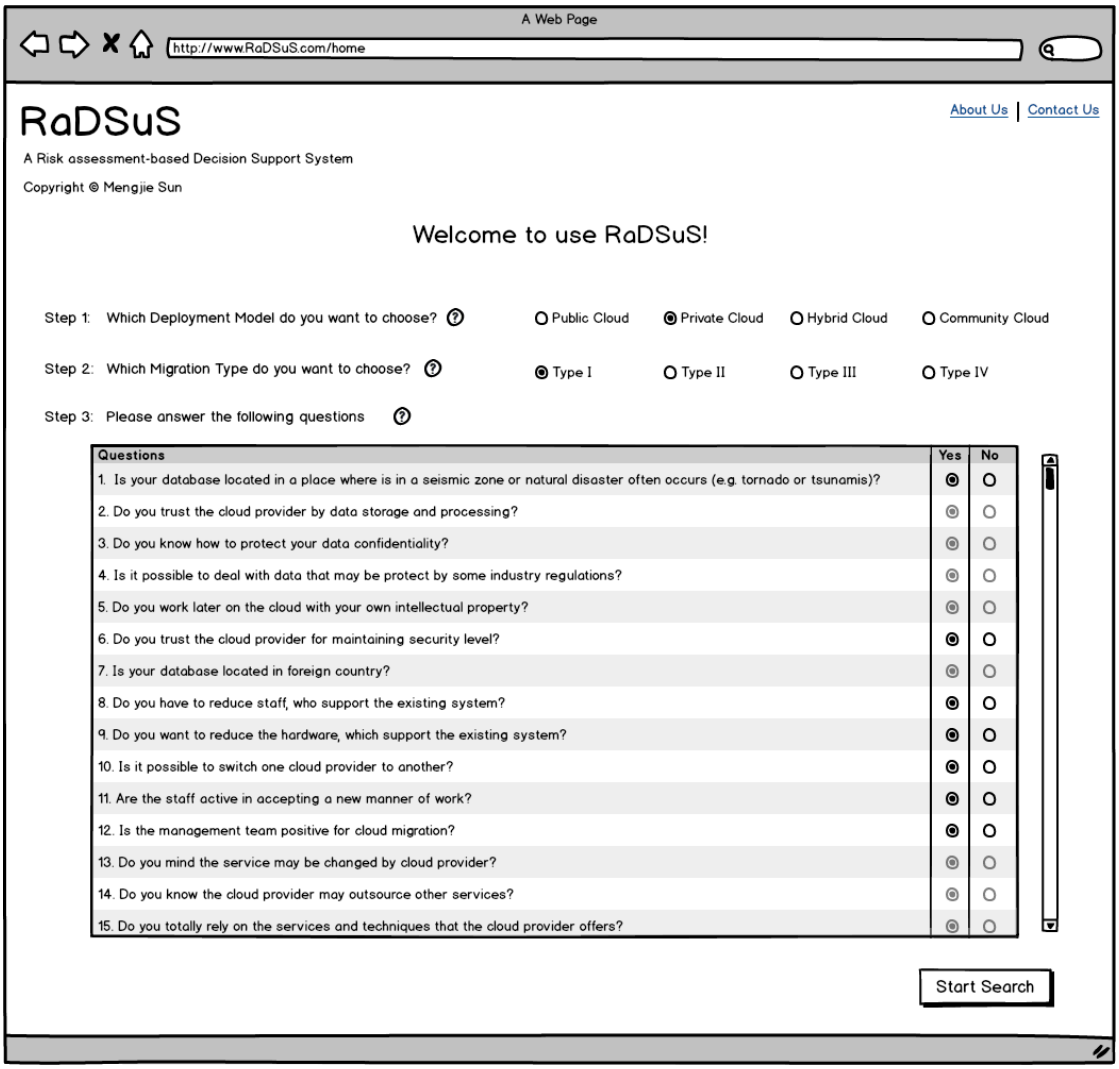


Figure 4.7: Questions when choosing Private Cloud and Migration Type I

When all 3 steps are finished, a search order will be submitted by clicking the Start Search button. Then the system will retrieve all the risks referring to the requirements and return a catalogue of risks with associated information. And the interface for displaying the results is activated, as shown in Figure 4.8. In this page the upper part is remained from the home page and the lower part is turned to a listing of result. The most important features of risks such as risk name, context of occurrence and risk mitigation methods are involved for presentation. In additional there is a button for a drop-down table of other attributes in the end of each risk column, as illustrated in Figure 4.9. Since there are all kinds of information in our risk catalogue and these should be shown optionally to meet the users requires.

As needed, the user can ask for a new search with changes of requirements by clicking the button New Search, which navigates users to go back to the home page of the system.

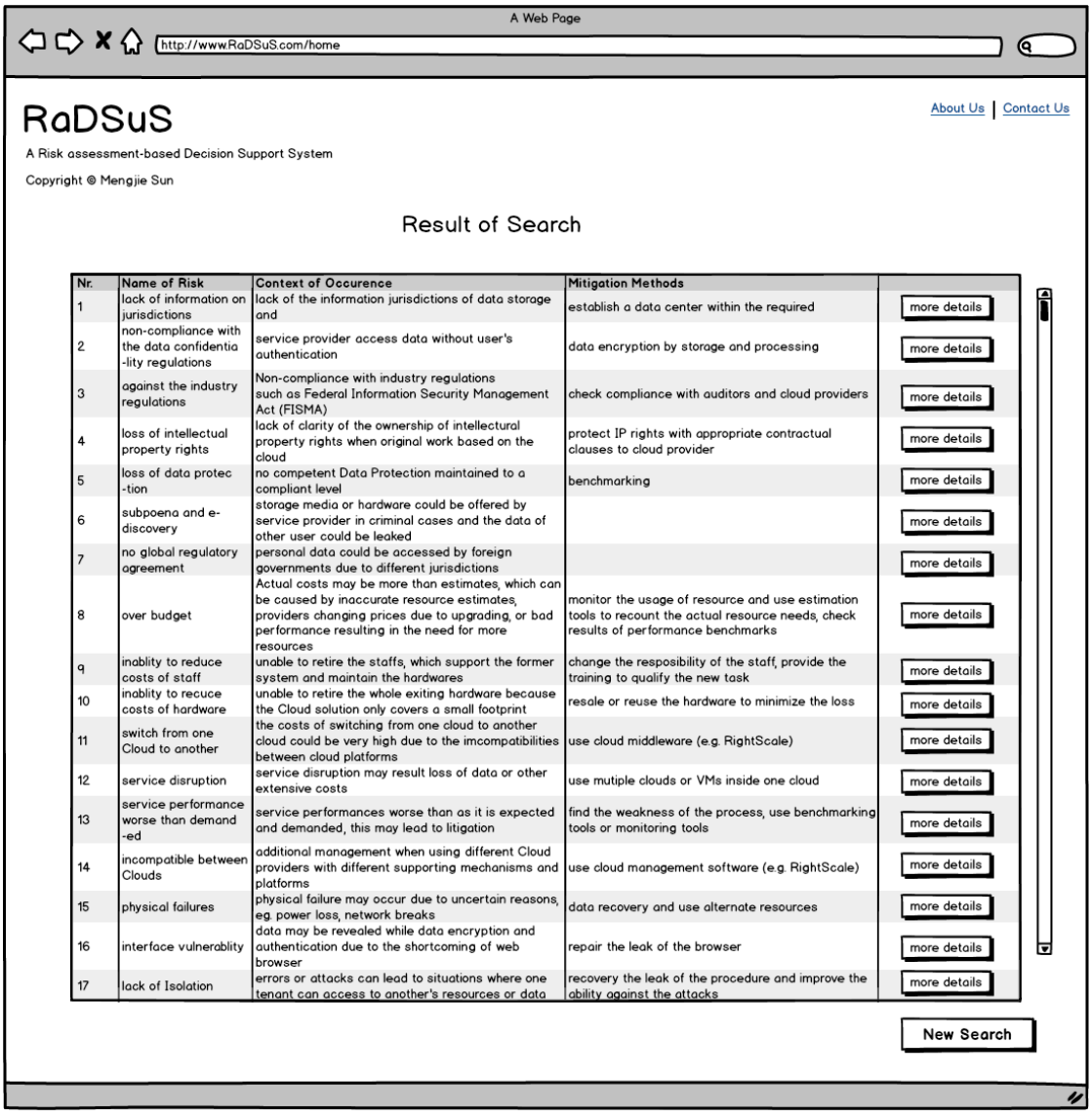


Figure 4.8: Result of the Risk Search

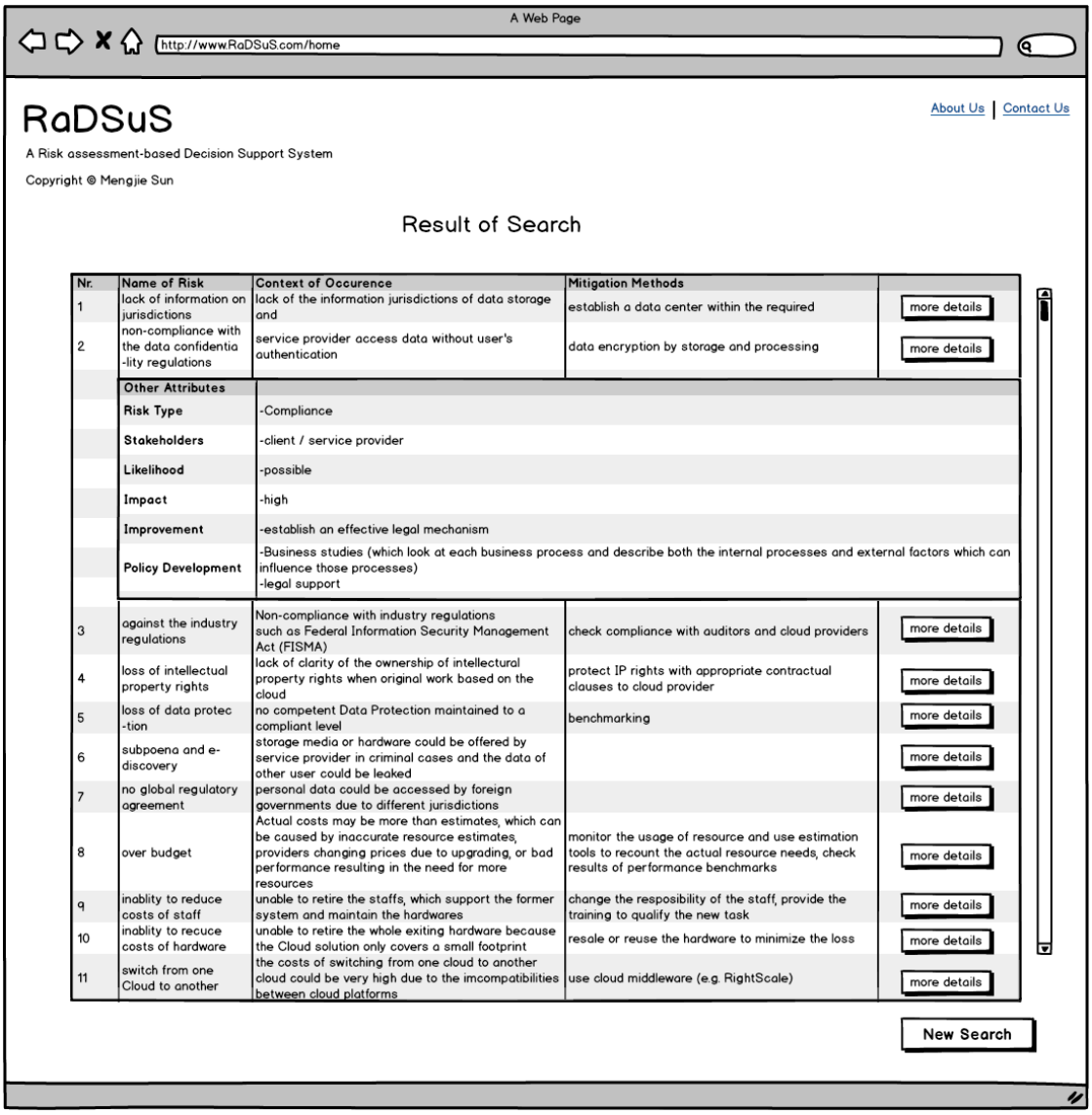


Figure 4.9: Other Attributes of the Risk

4.4 Implementation

This system is named RaDSuS that comes from the abbreviation of Risk assessment-based Decision Support System. It is developed on the Windows and run on the Tomcat. For the database layer, Postgresql is chosen due to its advantages in free-for-use and programmability. This system will be written in Java on the IDE Eclipse Kepler JEE and represented in HTML, JSP, JS and CSS. A structured illustration is shown in Figure 4.10

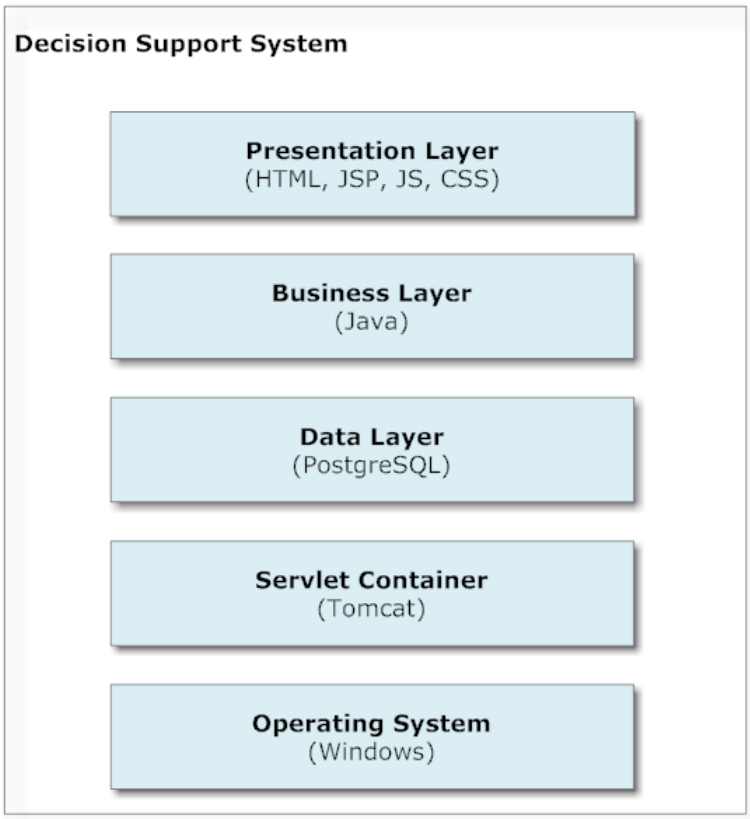


Figure 4.10: Layer Model with Implementaion

4.4.1 Risk database

In order to gain more scalability and save development and licensing costs, an open-source software solution is on demand for implementing database. PostgreSQL is an object-relational database management system with an emphasis on extensibility and standards compliance. The data queries can be easy realized by using SQL language as same as other common database systems, e.g. data are linked together with the Foreign Key. Moreover there are many high-quality GUI Tools available for PostgreSQL from both open source developers and commercial providers. Due to the stability as well as the programmability PostgreSQL is chosen for the database implementation of this system.

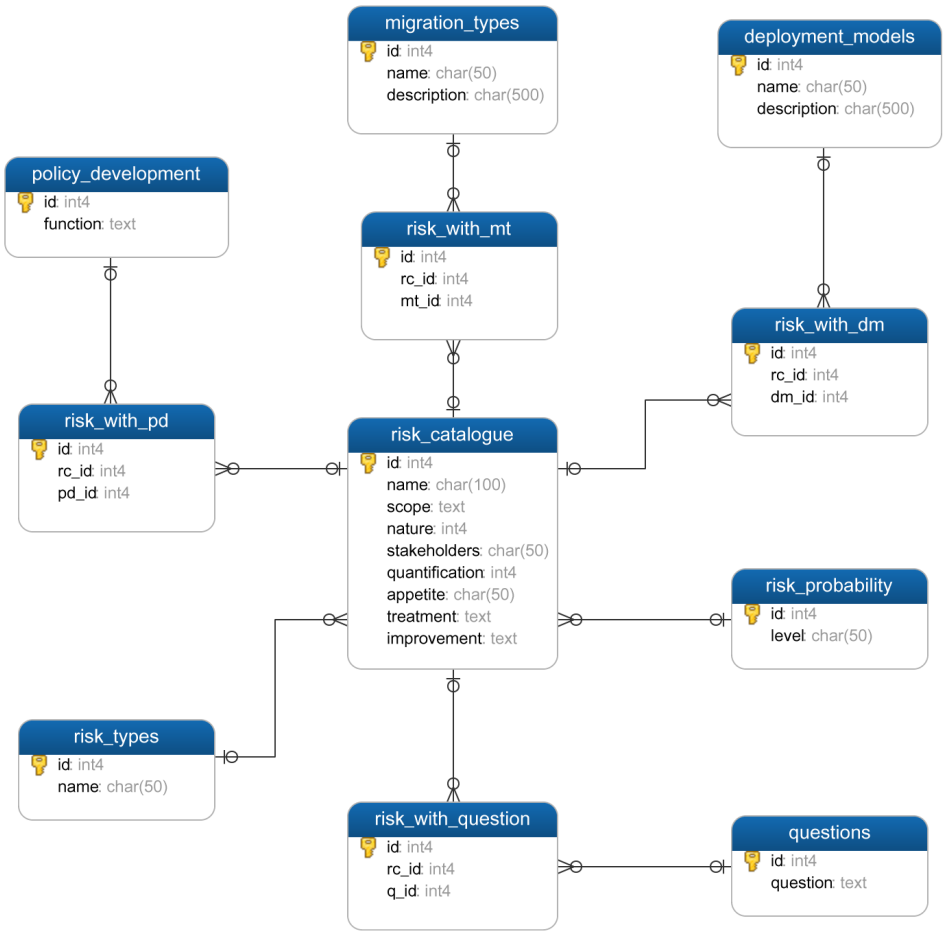


Figure 4.11: Data Model of Decision Support System

The risk database is implemented as a relational database on the basis of the corresponding ER model in Figure 4.2. And Figure 4.11 presents a data model of RaDSuS. This database consists of 11 entities. The entity risk_ catalogue acts as the basic element and all the other entities are direct or indirect related to it. There are 4 deployment models and 46 risks. Each model is related to different number of risks, which build totally 161 combinations of relations between these two entities. Similarly, 4 migration types build 77 combinations in all with 46 risks, since the migration type is supposed to be only related to those risks in *Knowledge Management*. Questions are used to identify other types of risks which has a one-to-many relationship with risk_ catalogue. Besides, the robability and types have both a one-to-many relationship with risk_ catalogue since each risk has only one risk type and one probability of occurrence. The id in risk_ probability and in risk_ type acts as foreign keys referencing to quantification and nature in risk_ catalogue.

4.4.2 RESTful Service

The new system is designed as a RESTful Web Service system. An open-source software Java EE is used for implementation due to its popularity. Java is aimed to be easy to use and is therefore much easier to learn and write than other programming languages. The most significant advantage of Java is its platform-independency, accompany with considering security and reliability. On the other side, there are many RESTful Web Services with large number of examples written in Java in the market. Therefore it is logical and reasonable to choose Java as the first choice of OOP to implement the system.

Since a Java platform has been determined, a suitable framework requires consideration. Restlet is a lightweight, comprehensive, open-source REST framework for Java platform and suitable for both server and client web applications. It supports major Internet transport and data format like HTTP and HTTPs, service description standards like XML and JSON. Certainly there are some other platforms in the market such as Jersey and Spring, which are with different advantages comparing to the Restlet and there are no evidence to prove which one is better. But we have chosen Restlet Framework to achieve all the RESTful Web Services in this work, which are exposed as RESTful APIs. Theses APIs are also be used in other systems with the same tasks like RaDSuS. Developing RESTful Web services in Java is very common and there are lots of tutorials or examples to show how to build RESTful APIs, such as the book from Manning [23], which is very helpful to this work.

REST consists of 3 ingredients: Resources, Representations and Interaction. Resource instance and collection facilitate interaction with multiple servers and a Restlet component is used as a container of Restlet applications or Servlet engine. In this work all the resources are identified by URIs and represented as XML and JSON. All Restlet applications are developed under separate URI paths, and Servlet engine is used to contain all these applications and to provide server HTTP connector. Finally a package of Servlet project will be done as a WAR file in order to support the system running in any environments by rebuilding the risk database from the data backup file.

All the URIs that are supported by RaDSuS are listed in Table 4.1. The system name radsus is used as the root directory. All these services are hosted on Tomcat and the default port is 8080. Each URI is mapping to 2 representations, XML and JSON, in which the contents are the same. All the contents of each URI are also presented in Table 4.1.

Table 4.1: Resource URIs supported by RaDSuS

URI (...=$http://localhost:8080/radsus$)	**XML/JSON Content**
$/deploymentModels$	deployment model
	URI of each deployment model
$/deploymentModels/\{modelName\}$	descriptions of each model
$/migrationTypes$	migration type
	URI of each migration type
$/migrationTypes/\{typeName\}$	descriptions of the each
$/questions$	questions about risks
	URI of each question
$/questions/question\_\{ID\}$	descriptions of the question
	corresponding risks of the question
	URI of each risk
$/riskTypes$	type name
	URI of each risk type
$/riskTypes/\{typeName\}s$	risks of each type
	URI of each risk
$/riskPolicy$	description of the policy
	URI of the policy
$/riskPolicys/policy\_\{ID\}$	description of the policy
	coresponding policy of the risk
	URI of each risk
$/risks$	risk name
	URI of each risk
$/risks/risk\_\{ID\}$	risk name
	risk scope
	stakeholders
	risk likelihood
	risk impacts
	risk treatment
	improvement
$/risksSearch?query$	risk names
	URI of each risk

4.4.3 User Interface

The frontend interface of RaDSuS is developed in JSP pages with using JS, CSS, JAVA and HTML. There are two pages implemented. The first page is designed for acquiring the users requirements with 3 steps. The first two steps are to determine the general environment of the cloud by selecting deployment model and migration type. Each step is accompanied with some hints in order to guiding the user how to choose. All these hints are implemented with dynamic table and designed as hidden information that is displayed by clicking the button with question mark. Because of the uniqueness by selecting deployment model and migration type, radio boxes are used to deliver the users choice to the RESTful services. The third step is designed for some experts or developers to identify some risks by answering specific questions with either yes or no, so the radio box is also used here as shown in the mockup figure in Section 4.3.3. Similar some hints are also given for step 3 with dynamic table and button.

The second page is to present the result by risk searching, when the system has identified all the risks according to the users requirements and returned risks found with related information through the RESTful services as well. Only the main information such as risk name, context of occurrence, and mitigation methods are displayed in this main page. By clicking the button more details the other features of risk are shown under each risk description which is implemented in the same way as the hints in the first page.

4.5 Summary

In this section, a risk assessment-based decision support system named RaDSuS is revealed from concept to implementation phrase. In the meantime, the requirements as well as the specifications of this system are firstly discussed, which include some details in function, interaction, data and system independence. Then a conceptual framework is given which consists of a UI as frontend and a database as Backend. ER-diagram and UI mockups are used to explain the structure of database and HMI. This system is designed as a RESTful Web Service system with implementation in JEE and represention in HTML, JSP, JS and CSS. All the resources are identified by URIs and represented as XML and JSON, while PostgreSQL is chosen to build a rational database of this system.

5 Evaluation

In this chapter, a set of use cases of cloud migration are collected to evaluate the usability of this decision support system. The evaluation of RaDSuS is realized by comparing to the risk occurrence from these use cases, which are cited from other documents and literatures where the possible risks are discussed and their scenarios are described.

All the information about use cases are presented in Appendix A.3. In the Table A.18 12 use cases are listed with its ID number, the problem accounts before and after cloud migration are briefly described, and the deployment model as well as the corresponding migration types are also concluded from the context. A general understanding of each case is therefore in available. In additional Table A.19 summarizes the all the risks of these 12 use cases with a checking table in order to get a clear contrast.

Use case 3 (U3) that is from the research by Khajeh-Hosseini et al. [24] will be taken at first on discussion. The case study organization is a UK based SME (company B) that provides bespoke IT solutions for the Oil & Gas industry. Company B provides a system, which consists of a database server and an application server, for company C as an end user to address company A. Now a requirement in moving the quality monitoring and data acquisition system to Amazon EC2 is on demand. According to this article, a public cloud is chosen with migration type I or type II. Table 5.1 gives a comparison on risks identified by other related work from David Greenwood [25] and by the system.

From the table we can find out that all the risks referred in the article are included in the searching field of the system result, which validates the correctness of risk searching to a certain extent. Some types of risks such as financial are not mentioned in these two cited articles, which doesnt mean this type of risks are not exiting in this case. It is only because these risks may be not the key risks in these articles or beyond their discussions. Similar some risks such as R38 is one of the risks from system result but not in U3, which means R38 should also be occur in U3 and merely there is no referring in this cases description.

According to the working process of system, some risks like R1 are removed from the searching field after choosing the public cloud for user requirements. Then the migration type is chosen, which will go on narrowing the searching field. We have to omit the questionnaire phase in this test because we are supposed to have no specific requirements and aiming to find all the possible risks. Since no questions are answered, the system takes the default answer of yes and returns all the corresponding risks. Finally all the risks are revealed in the row of “Result of RaDSuS.

Table 5.1 lists 2 rows of system result due to the two migration types. By comparison of these two results we find that they are differing in the type Knowledge Management, e.g. R15 occurs with migration type II but not with migration I, as same as R21. This

can prove from the other side that migration type I is with less risks than migration type II.

	Risks				
	Compliance	**Financial**	**Knowledge Management**	**Operational**	**Strategic**
Use Case 3 (public cloud & migration type I / II)	R44	not mentioned	R13, R14, R16, R19, R22, R23, R25	R32, R33, R34	R42
Result of RaDSuS with migration type I	R2, R3, R4, R5, R6, R7, R8, R44	R9, R10, R11, R12	R13, R14, R16, R17, R18, R19, R22, R23, R24, R25, R26, R27, R28, R29, R30, R31, R43	R32, R33, R34, R35, R36, R37	R38, R39, R40, R41, R42
Result of RaDSuS with migration type II	R2, R3, R4, R5, R6, R7, R8, R44	R9, R10, R11, R12	R13, R14, R15, R16, R17, R18, R19, R21, R22, R23, R24, R25, R26, R27, R28, R29, R30, R31, R43	R32, R33, R34, R35, R36, R37	R38, R39, R40, R41, R42

Table 5.1: Risks in Use Case 3 comparing with RaDSuS result

We use U6 as the second example that is from another work by Khajeh-Hosseini et al. [8]. From its description the School of Computer Science at University of St. Andrews has five full-time system administrators that maintain its relatively complex IT infrastructure. The schools computing services that involve storage and network services are currently deployed on 28 application servers and 5 storage servers locally with 5 full-time system administrators and 200 desktop machines which are needed to be upgraded. After comprehensive analysis and discussion services are deployed on 9 application servers and 3 storage servers, however some services like network monitoring service are proved to be not suitable for cloud migration. Therefore the best solution is to purchase physical servers and build up their own computing center. From this context a private cloud has been chosen and the migration type is concluded in Type II. All the possible risks according to the document context are listed in Table 5.2, which provides a comparison concerning risks with the system result.

From the result we find out that all the risks identified in the article are included in the system result, not even a risk is beyond this field. Some type of risks such as compliance and strategic are not mentioned in the document. The system returns all the risks as default because of no answer given in the question phase. Certainly when the user could give more information by answering questions, this system can be more powerful and

	Risks				
	Compliance	**Financial**	**Knowledge Management**	**Operational**	**Strategic**
Use Case 6 (public cloud & migration type II)	not mentioned	R9, R11	R13, R16, R21, R25, R31	R32	not mentioned
Result of RaDSuS	R1, R6, R7	R9, R10, R11, R12	R13, R16, R17, R21, R23, R24, R25, R27, R29, R30, R31, R43	R32, R33	R38, R40, R42

Table 5.2: Risks in Use Case 6 comparing with RaDSuS result

specific in risk identification. And we also learned from the table that private cloud has less risks than public cloud when using cloud service.

U1 will be taken as the third example, which described by Microsoft team [4]. In this case the IT department for Department of Citizen Engagement (DoCE) wants to move its email system, which consists of several email systems from same vendor but of varying generations, to a single, consolidated platform to remain 'ever green' and keep flexible on delivery of varying devices and channels. After investigation a hybrid cloud is chosen for implementation with migration type II. Table 5.3 lists the risks identified in the literature in comparison with the 43 risks from the result of the system.

	Risks				
	Compliance	**Financial**	**Knowledge Management**	**Operational**	**Strategic**
Use Case 1 (hybrid cloud & migration type II)	R1, R2, R3, R6, R7	not mentioned	R13, R15, R18, R19, R21, R22, R27, R28, R30, R31, R43	R37	R38, R41, R42
Result of RaDSuS	R1, R2, R3, R4, R5, R6, R7, R8, R44	R9, R10, R11, R12	R13, R14, R15, R16, R17, R18, R19, R21, R22, R23, R24, R25, R26, R27, R28, R29, R30, R31, R43	R32, R33, R34, R35, R36, R37	R38, R39, R40, R41, R42

Table 5.3: Risks in Use Case 1 comparing with RaDSuS result

We take U2 as the fourth case. This case is cited by Sailesh Gadia [26], which describes a company A that offers BusinessExpress as a Software as a Service and is planning to use IaaS for a hosting solution. In this case a public cloud is chosen with migration type IV. All the results are presented in Table 5.4.

	Risks				
	Compliance	**Financial**	**Knowledge Management**	**Operational**	**Strategic**
Use Case 1 (public cloud & migration type IV)	R2, R3, R4, R6, R44	not mentioned	R14, R17, R23, R24, R28	not mentioned	R38, R39, R41, R42
Result of RaDSuS	R2, R3, R4, R5, R6, R7, R8, R44	R9, R10, R11, R12	R13, R14, R15, R17, R18, R19, R20, R21, R22, R23, R24, R25, R26, R27, R28, R29, R30, R31, R43, R46	R32, R33, R34, R35, R36, R37	R38, R39, R40, R41, R42

Table 5.4: Risks in Use Case 2 comparing with RaDSuS result

From all these 4 use cases we could learn that the system returns all the possible risks with different amount due to different deployment models and different migration types, when no questions are used for identification of specific risks. Hybrid cloud is with more risks than public cloud and private cloud, while migration type I is with the least risks in comparison with other types, which are also consistent with the definitions and descriptions of deployment models and migration types. This system is proved to be able to show all the related risks after collecting the users requirements such as choosing deployment model and migration type. More accurate searching will be achieved if more information is given in the questionnaire phase. And the system can be verified certainly with other use cases in Appendix A.3 as well.

6 Conclusions

6.1 Summary

With the development of IT techniques and growing amount of researches and reports we gradually realize that cloud computing pose a both an opportunity and a challenge for enterprises. It benefits the cloud users by offering an efficient on-demand service and enables enterprises to pay more attentions to developing business instead of investment, setup and maintain their own hardware. With the advantages in scalability, high-level-availability, flexibility and easy-using cloud computing is now evolving like never before, with enterprises of all types and scales adapting to this new technology. However the security issues should be undoubtedly considered since many use cases evidence that there are certain issues and problems accompanied with those advantages. It is very helpful to recognize the risks associated as much as possible before determining migrating to the cloud. Therefore a comprehensive understanding of risks that may be confronted is quite important for a rational decision. Furthermore an easy using decision support system based on risk assessment is also proposed in this work.

To achieve our goals, some related works have been first referred to, which involves the basic knowledge about cloud computing and decision support system for cloud migration. Then we have discussed the risk management issues and learned the standards of risk definition by IRM, which is as the basis of our new catalogue of risks that may occur by applications adoption to the cloud. By referencing a quantity of scientific documents and technical reports as well as many case studies, a list of risks are identified and adapted into this new catalogue with full-detailed information, which are presented in Appendix A.2

In order to simplify the recognition of all risks, a decision support system as an intuitive method has been proposed instead of traditional workshop or arrangement meeting. This user-friendly system named RaDSuS is targeted on showing all the possible risks that the user might confront, with satisfying the users requirements by choosing deployment model and migration type as well as answering some specific questions. This system is designed as a RESTful Web service, by which all the resources are identified by URIs and represented as XML and JSON data format. The user interface of this system acts as frontend which is built on JSP with Servlet, while a rational risk database structured in PostgreSQL as backend.

To evaluating the ability of risk searching, a number of use cases listed in Appendix A.3 are applied, which are with different deployment models and migration types. In comparing with the results in Table A.19, RaDSuS are proved to be able to specify the users requirements and give the decision maker a general understanding of all risks associated by cloud migration.

6.2 Future Work

Although we have redefined all the risks with the IRM standard of risk description and successfully applied it into a new decision support system for risk assessment, there are still some limitations of the catalogue as well as the system themselves and some improvement can be also recommended in the future work.

- The risk catalogue classifies all the 46 risks in 5 categories. However the risks in type *Knowledge Management* are in the majority comparing to other types of risks, e.g. there are only 5 risks in *Strategic* and 4 in *Financial*. It is strongly advised to subdivide this category *Knowledge Management* into such as knowledge concerning and technique implemental, in order to get a better understanding of when and where the risks may occur.
- This catalogue summarizes all the risks according to large amount of references and case studies and identifies risk in a general art of definition, i.e. some risks are generalized as one risk. So it is relative difficult to address the risks to the migrating components, by which we implement in our system with some specific questions. It could be accomplished in a proceeding work of research.
- The decision support system aims to return all the possible risks with detailed information for a general understanding according to the requirement of this thesis, but with no needs to score and rank of risks. There are lots of researches on how to assess and evaluate the risks with weights and in this work we have also identified the likelihood and impact with some scores. With these factors we could list all the risks with some specific requirements such as displaying top 10 risks with largest impacts or listing top 5 risks in particular risk type in the future work.

Appendix

A.1 Strategy and Policy Developments

Table A.1: Strategy and Policy Developments

ID	Strategy and Policy Developments
F1	Auditing and inspection
F2	Brainstorming
F3	Business studies (which look at each business process and describe both the internal processes and external factors which can influence those processes)
F4	Hazard & Operability Studies
F5	Incident investigation
F6	Industry benchmarking
F7	Interview and questionnaires
F8	Legal support
F9	Scenario analysis
F10	Technical training
F11	Use Case study

A.2 Risk Description

Table A.2: Risk Description

ID	Name of Risk	Scope of Risk	Nature of Risk	Stakeholders	Quantification of Risk
R1	natural disaster	hardware and data can be damaged by natural disaster or fire	Compliance	CC / SP	very unlikely
R2	lack of information on jurisdictions	lack of the information jurisdictions of data storage and processing	Compliance	SP	unlikely
R3	non-compliance with data confidentiality regulations	service provider access data without user's authentication	Compliance	CC / SP	possible
R4	against the industry regulations	Non-compliance with industry regulations, such as Federal Information Security Management Act (FISMA)	Compliance	SP	possible
R5	loss of intellectual property rights	lack of clarity of the ownership of intellectural property rights when original work based on the cloud	Compliance	CC	possible
R6	loss of data protection	no competent data protection maintained to a compliant level	Compliance	SP	possible
R7	Subpoena and e-discovery	storage media or hardware could be offered by service provider in criminal cases	Compliance	SP	likely

Table A.3: Risk Description - continued

Risk Tolerance /Appetite	Risk Treatment & Control Mechanisms	Potential Action for Improvement	Strategy and Policy Development	Reference
high	data duplicated for a backup in other locations		F4	[3] [4]
high	establish a data center within the required jurisdictions		F8	[27] [28]
high	data encryption by storage and processing	establish an effective legal mechanism	F3, F8	[27] [29] [30] [31]
high	check compliance with auditors and cloud providers		F8	[30] [27] [32]
high	protect IP rights with appropriate contractual clauses to cloud provider		F8, F10	[3] [27]
high	no competent Data Protection maintained to a compliant level	keep competitive in data protection technology and benchmarking	F6	[4] [32] [26]
medium			F8	[3] [4]

Table A.4: Risk Description - continued

ID	Name of Risk	Scope of Risk	Nature of Risk	Stakeholders	Quantification of Risk
R8	no global regulatory agreement	personal data could be accessed by foreign governments due to different jurisdictions	Compliance	SP	very likely
R9	over budget	Actual costs may be more than estimates, which can be caused by inaccurate resource estimates, providers changing prices due to upgrading, or bad performance resulting in the need for more resources	Financial	CC / SP	possible
R10	inablity to reduce costs of staff	unable to retire the staffs, which support the former system and maintain the hardwares	Financial	CC	likely
R11	inablity to recuce costs of hardware	unable to retire the whole exiting hardware because the Cloud solution only covers a small footprint	Financial	CC	possible
R12	switch from one Cloud to another	the costs of switching from one cloud to another cloud could be very high due to the imcompatibilities between cloud platforms	Financial	CC	possible

Table A.5: Risk Description - continued

Risk Tolerance /Appetite	Risk Treatment & Control Mechanisms	Potential Action for Improvement	Strategy and Policy Development	Reference
high		establish global regulatory agreement with full transparency	F8	[32] [4]
medium	monitor the usage of resource and use estimation tools to recount the actual resource needs, check results of performance benchmarks	analyse and plan clearly and detailed before migration for the actual need of the service	F1, F3, F6	[8] [29]
medium	change the resposibility of the staff, provide the training to qualify the new task	make a well-considered strategy before migration with thinking of the cost of human resources	F2, F6, F7	[33] [34] [35]
low	resale or reuse the hardware to minimize the loss	investigate and reserch detailly before migration	F4	[33]
high	use cloud middleware (e.g. RightScale)		F1, F4, F11	[36]

Table A.6: Risk Description - continued

ID	Name of Risk	Scope of Risk	Nature of Risk	Stakeholders	Quantification of Risk
R13	service disruption	service disruption may result loss of data or other extensive costs	Knowledge Management	SP	possible
R14	worse service performance	service performances worse than as it is expected or demanded, which may lead to litigation	Knowledge Management	CC / SP	possible
R15	incompatible between Clouds	extra management when using different Cloud providers with different supporting mechanisms	Knowledge Management	SP	likely
R16	physical failures	physical failure may occur due to uncertain reasons, eg. power loss, or network breaks	Knowledge Management	CC / SP	possible
R17	interface vulnerablity	data may be revealed while data encryption and authentication due to shortage of web browser	Knowledge Management	CC	possible
R18	lack of Isolation	errors or attacks can lead to situations where one tenant can access to another's resources or data	Knowledge Management	SP	possible
R19	Data Lock-in	Data lock-in for SaaS /Paas	Knowledge Management	SP	likely

Table A.7: Risk Description - continued

Risk Tolerance /Appetite	Risk Treatment & Control Mechanisms	Potential Action for Improvement	Strategy and Policy Development	Reference
high	use multiple clouds or multiple VMs inside one cloud	monitor the applications from outside and prevent a disruption in advance	F4, F5	[24] [37] [38] [39]
medium	lack of the information jurisdictions of data storage and processing	an independent auditor's report regarding the state of controls of SP needs to be reviewed	F3, F5, F6	[37] [38] [40] [41] [26]
low	use cloud management software (e.g. RightScale)	establish a standardization between cloud providers	F4	[10] [21]
medium	data recovery and use alternate resources		F4, F11	[37]
high	repair the leak of the browser	browser regular update for precaution	F5	[42] [43]
high	recovery the leak of the procedure and improve the ability against the attacks		F3, F6, F9	[3] [44]
medium	agreement in standardization among the cloud providers		F3, F6, F8	[3] [38] [36]

Table A.8: Risk Description - continued

ID	Name of Risk	Scope of Risk	Nature of Risk	Stakeholders	Quantification of Risk
R20	licensing Issues	software licenses are unusable on the cloud because of the traditional licensing agreements	Knowledge Management	CC / SP	unlikely
R21	mismatched infrastructure	the exiting procedure is not suitable for the Cloud procedure, over-provisioned or unter-provisioned	Knowledge Management	CC / SP	likely
R22	malicious activities	malicious activities on the system from cloud provider insider or co-tenants,such as spamming, port scanning and crashing servers	Knowledge Management	CC	possible
R23	degradation of network performance	network performance could be worse over time with more and more users start to use cloud	Knowledge Management	CC	possible
R24	simple accessing mechanism	data may be leaked due to simple access mechanism, such as using only username/password login mechanism to access personal data	Knowledge Management	SP	possible

Table A.9: Risk Description - continued

Risk Tolerance /Appetite	Risk Treatment & Control Mechanisms	Potential Action for Improvement	Strategy and Policy Development	Reference
medium	check all software license agreements		F5	[45]
high	reanalyse the business process and reclassify the procedure	ensure that the provide's SLA are well defined and procedure clearly classified before migration	F3, F5	[3] [37] [46]
medium	find benchmarking service provider and follow best practices, such as microsoft or AWS		F6, F10	[4] [5]
medium	use monitoring tools outside the cloud	a duplicated system on another cloud is standby	F3, F5	[47] [5]
high	use additional mechanisms to restrict access, such as multi-factor authentication by AWS		F6, F11	[5]

Table A.10: Risk Description - continued

ID	Name of Risk	Scope of Risk	Nature of Risk	Stakeholders	Quantification of Risk
R25	lack of knowledge of cloud concerns	inefficiency or incompetence of work, or data leakage with wrong operation due to lack of cloud knowledge	Knowledge Management	CC	possible
R26	lack of technological competitiveness	service provider lags in technology improvement and not keep-up with the development	Knowledge Management	SP	unlikely
R27	social engineering attacks	manipulate people into performing illegal actions or divulging confidential information	Knowledge Management	SP	likely
R28	intercepting data in transfer	API messages and data could be intercepted in transit, especially in shared environments and transfering data between client and provider	Knowledge Management	CC / SP	likely
R29	insecure deletion of data	unencrypted data could still be accessed and recovered after deletion from the user	Knowledge Management	CC	possible

Table A.11: Risk Description - continued

Risk Tolerance /Appetite	Risk Treatment & Control Mechanisms	Potential Action for Improvement	Strategy and Policy Development	Reference
high	train the users with corresponding knowledge such as how and which types of data they can put on the public cloud		F10	[24]
medium	keep competitive in technology development and benchmarking		F6, F10	[7] [24]
high			F8, F11	[3] [48]
high	data encryption by storage and processing	data transit with a secure channel such as Secure Sockets Layer (SSL) or Secure Shell (SSH)	F6	[10] [30] [26]
high	data encryption by storage and processing, use special procedures to delete data		F10	[3] [48]

Table A.12: Risk Description - continued

ID	Name of Risk	Scope of Risk	Nature of Risk	Stakeholders	Quantification of Risk
R30	loss of backups of user	data backups of the user made by service provider could get damageed, lost or stolen	Knowledge Management	SP	unlikely
R31	denial-of-service attracks	a flood of attacks sending a huge amount of nonsense requests to a certain service can cause a denial of service to the server hardware	Knowledge Management	SP	possible
R32	reduction of productivity	changing the former working manner can make the staff getting less satisfaction and reduce productivitiy by using cloud infrastructure	Operational	CC	possible
R33	resistance from the staff	Migration may be resisted by the organizational politics or labor union	Operational	CC	possible
R34	changes of composition of provider	service may be changed because of the changes of composition by cloud provider	Operational	SP	possible

Table A.13: Risk Description - continued

Risk Tolerance /Appetite	Risk Treatment & Control Mechanisms	Potential Action for Improvement	Strategy and Policy Development	Reference
high			F10, F11	[3]
high	use network monitoring tools from outside of the cloud		F5, F9, F11	[29] [42] [49]
low	ensure that they won't be dismissed and provide the training course to qualify them to the new task	give the staff more positive information and arouse the enthusiasm of the new manner of working before migration	F2, F7	[24] [50]
low	inform the advantages of the new technique and comfirm the staff to a better further, involve key stakeholders in the adoption process	a communicate with stakeholders, hear the opinion and advices and make a common plan before migration	F2, F7	[24] [51]
medium	use multiple providers		F4	[3] [48]

Table A.14: Risk Description - continued

ID	Name of Risk	Scope of Risk	Nature of Risk	Stakeholders	Quantification of Risk
R35	supply chain failure	A provider can outsource parts of its production chain to third parties, or even use other providers as part of its service, a potential cascading failures is created	Operational	SP	unlikely
R36	loss of innovative ability	the user relies tatally on the cloud provider when using SaaS and is not willing to learn or innovate	Operational	CC	possible
R37	out of business by cloud provider	cloud provider could be out of business or merged by another company	Operational	SP	possible
R38	lack of standards	cloud services market lacks widely accepted standards for availability and interoperability and may cause legal dispute later	Strategic	SP	unlikely
R39	loss of governance and control of resource	the roles and responsibilities after migration are not clear identified	Strategic	CC	likely
R40	change of cloud service	customer may change cloud service with other strategy	Strategic	CC	unlikely
R41	poor provider selection	selection of service provider may result in system operational degradation	Strategic	CC	unlikely

Table A.15: Risk Description - continued

Risk Tolerance /Appetite	Risk Treatment & Control Mechanisms	Potential Action for Improvement	Strategy and Policy Development	Reference
medium	use multiple providers		F4	[21] [3]
medium	improve the initiative of the stuff, organisational learning		F2, F10	[5] [52]
high	use multiple providers	backup data outside of the cloud	F4, F11	[53]
medium	service provider benchmarking	establish a well accepted industry standard	F6, F11	[32] [54]
high	make sure the contract specifies, guarantee hold intellectual of the information	clarify roles and responsibilities before migration	F3, F8	[24] [21] [55]
high	clarify the strategy before cloud migration considering of further development		F3, F4	[56]
medium	select benchmarking service provider		F6, F11	[4]

Table A.16: Risk Description - continued

ID	Name of Risk	Scope of Risk	Nature of Risk	Stakeholders	Quantification of Risk
R42	loss of business reputation	loss of business reputation due to bad performance by cloud adoption	Strategic	CC	possible
R43	logs & tracing failure	loss or compromise of operational Logs (including security Logs)	Knowledge Management	SP	unlikely
R44	contract issues	the contract between CC and SP does not include certain critical elements to help protect security and privacy requirements	Compliance	CC / SP	likely
R45	VM breakdown	virtual resource breakdown	Knowledge Management	SP	possible
R46	system lock-in	system lock-in for IaaS	Knowledge Management	SP	likely

Table A.17: Risk Description - continued

Risk Tolerance /Appetite	Risk Treatment & Control Mechanisms	Potential Action for Improvement	Strategy and Policy Development	Reference
high	comprehensive research and investigation on cloud providers before migration		F6, F11	[4] [5]
high	application teams manage the configuration of the cloud firewall instead of relying on network engineering team		F6	[4] [26]
high	establish contract with SP, which should include responsibilities, policies and standards in legal,security and privacy aspects		F8	[26] [25]
medium	use alternate resources		F4, F11	[37]
medium	use middleware that is compatible with multiple clouds for IaaS lock-in		F3, F6, F8	[38] [3]

A.3 Use Cases of Cloud Migration with Risks

Table A.18: Use Cases of Migration

ID	Application	Initial Topology	Migrated Topology	Deployment Model	Migration Type	Reference
U1	Department of Citizen Engagement (DoCE)	the email system consists of several separate email systems from same vendor but of varying generations	move the email system to a single, consolidated platform and provide flexibility of delivery to varying devices and channels	hybrid	I	[4]
U2	Company A	provides a SaaS service	uses IaaS for a hosting solution	public	IV	[26]
U3	Company B (IT solution for an oil and gas company)	Company B provides a system, which consists of a database server and an application server, for Company C as end users to address Company A	migrate quality monitoring and data acquisition system to Amazon EC2	public	I / II	[24] [25]
U4	University of Birmingham		outsources email service to the cloud	public	I/II	[57]
U5	Children's charity	hosted on an agency that provides a shared environment	move the website and some business applications into an hybrid platform cloud	hybrid	II	[54]

Table A.18 – continued from previous page

ID	Application	Initial Topology	Migrated Topology	Deployment Model	Migration Type	Reference
U6	The school of computer science (University of St Andrews)	computing services (common services, storage and network services) are deployed locally on 28 application servers and 5 storage servers with 5 full-time system administrators, 200 desktop machines which are needed to be upgraded	services are deployed on 9 application servers and 3 storage servers, some services (e.g. network monitoring service) are not suitable for migration by using Amazon S3, purchase physical servers	private	II	[8]
U7	mobile cloud e-health application		a scalable real-time halth monitoring and analysis system, transit data via bluetooth, use Amazon S3 for storage	public	I	[58]
U8	Entertainment Company		deals with single-player games and multiplayer games across multiple cloud platforms	public	I	[59]
U9	Army Experience Center	traditional environment, 21 fragmented email systems	choose a commercially-available SaaS solution for Customer Relationship Management system	private	II	[60]

Table A.18 – continued from previous page

ID	Application	Initial Topology	Migrated Topology	Deployment Model	Migration Type	Reference
U10	an insurance Company		use computing ability of public cloud, which deliver VMs to process enormous load of information	public	III	[61]
U11	an online retailer		develop new Web 2.0 storefront application with hosted developer tooling and a source code repository on one cloud, choose another cloud provider for testing	public	I/II	[61]
U12	a financial investment company		use cloud storage provider to scale the secure hosting and streaming of videos	public	I	[61]

Table A.19: Use Cases with Risks

Risk	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10	U11	U12
R1	x											
R2	x	x					x					
R3	x	x		x								x
R4		x		x					x			
R5												
R6	x	x		x					x	x		x
R7	x				x							
R8				x			x					
R9				x	x	x						
R10									x			
R11						x			x			
R12								x				
R13	x		x		x	x	x		x	x		
R14		x	x	x	x		x				x	
R15	x							x			x	
R16			x			x	x		x		x	x
R17		x					x					
R18	x											
R19	x		x		x				x			
R20								x	x			
R21	x					x		x	x			
R22	x		x									
R23		x	x	x	x		x					
R24		x		x						x	x	x
R25			x	x	x	x		x				
R26					x				x			
R27	x											
R28	x	x			x		x			x		x
R29										x	x	
R30	x			x	x							
R31	x				x	x						
R32			x		x	x						
R33			x									
R34			x	x								
R35				x								
R36								x				
R37	x											
R38	x	x		x	x				x			x
R39		x		x								
R40												
R41	x	x		x								
R42	x	x	x					x				
R43	x											
R44		x	x	x	x							
R45										x		
R46		x										

Bibliography

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, pp. 50–58, Apr. 2010.

[2] L. Zhou, "Cloudftp: A case study of migrating traditional applications to the cloud," in *Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on*, pp. 436–440, 2013.

[3] E. Network and I. S. Agency, "Cloud computing: benefits, risks and recommendations for information security," tech. rep., December 2012.

[4] P. N. Greg Stone, "Cloud risk decision framework: Principles risk-based decisionmaking for cloud-based computing derived from iso 31000." `http://download.microsoft.com/documents/australia/enterprise/SMIC1545_PDF_v7_pdf.pdf`.

[5] PlanForCloud.com, "Spreadsheet - benefits and risks of using the cloud." `http://blog.planforcloud.com/2012/02/the-benefits-and-risks-of-using-cloud.html`.

[6] IRM, "A risk management standard," *The Institute of Risk Management, London*, 2002.

[7] A. Khajeh-Hosseini, I. Sommerville, J. Bogaerts, and P. Teregowda, "Decision support tools for cloud migration in the enterprise," in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, pp. 541–548, IEEE, 2011.

[8] A. Khajeh-Hosseini, D. Greenwood, J. W. Smith, and I. Sommerville, "The cloud adoption toolkit: supporting cloud adoption decisions in the enterprise," *Software: Practice and Experience*, vol. 42, no. 4, pp. 447–465, 2012.

[9] V. Andrikopoulos, S. Strauch, and F. Leymann, "Decision support for application migration to the cloud: Challenges and vision," in *Proceedings of the 3rd International Conference on Cloud Computing and Service Science, CLOSER 2013, 8-10 May 2013, Aachen, Germany*, pp. 149–155, SciTePress, 2013.

[10] D. Catteddu, *Cloud Computing: benefits, risks and recommendations for information security*. Springer, 2010.

[11] P. Mell and T. Grance, "The nist definition of cloud computing (draft)," *NIST special publication*, vol. 800, no. 145, p. 7, 2011.

[12] C. S. Alliance, "Security guidance for critical areas of focus in cloud computing." `http://www.cloudsecurityalliance.org/guidance/csaguide.pdf`, 2009.

[13] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, "Cloud computing synopsis and recommendations," *NIST special publication*, vol. 800, p. 146, 2012.

[14] Techopedia, "Definition of cloud migration." `http://www.techopedia.com/definition/26440/cloud-migration`, November 2013.

[15] M. Fowler, *Patterns of enterprise application architecture*. Addison-Wesley Longman Publishing Co., Inc., 2002.

[16] V. Andrikopoulos, T. Binz, F. Leymann, and S. Strauch, "How to adapt applications for the cloud environment," *Computing*, vol. 95, no. 6, pp. 493–535, 2013.

[17] R. Economy and L. U. Programme, "Stakeholder impact analysis matrix." `http://www.relu.ac.uk/research/Innovation%20in%20Prog%20Management/SIAM.html`, November 2012.

[18] K. Djemame, D. Armstrong, M. Kiran, and M. Jiang, "A risk assessment framework and software toolkit for cloud service ecosystems," in *CLOUD COMPUTING 2011, The Second International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 119–126, 2011.

[19] International Organization for Standardization, "Iso 31000:2009 risk management – principles and guidelines." `http://www.iso.org/iso/catalogue_detail?csnumber=43170`, 2009.

[20] Enterprise Risk Management Committee *et al.*, "Overview of enterprise risk management," in *Casualty Actuarial Society*, 2003.

[21] J. Dibbern, T. Goles, R. Hirschheim, and B. Jayatilaka, "Information systems outsourcing: a survey and analysis of the literature," *ACM SIGMIS Database*, vol. 35, no. 4, pp. 6–102, 2004.

[22] S. C. University, "Risk treatment." `http://scu.edu.au/risk_management/index.php/6`.

[23] J. Louvel, T. Templier, and T. Boileau, *Restlet in Action: Developing RESTful Web APIs in Java*. Manning, 2012.

[24] A. Khajeh-Hosseini, D. Greenwood, and I. Sommerville, "Cloud migration: A case study of migrating an enterprise it system to iaas," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pp. 450–457, IEEE, 2010.

[25] D. Greenwood and I. Sommerville, "Responsibility modeling for identifying sociotechnical threats to the dependability of coalitions of systems," in *System of systems engineering (SoSE), 2011 6th international conference on*, pp. 173–178, IEEE, 2011.

[26] A. C. C. Sailesh Gadia, CISA, "Cloud computing risk assessment: A case study," *ISACA*, vol. 4, 2011.

[27] A. Joint, E. Baker, and E. Eccles, "Hey, you, get off of that cloud?," *Computer Law & Security Review*, vol. 25, no. 3, pp. 270–274, 2009.

[28] P. T. Jaeger, J. Lin, J. M. Grimes, and S. N. Simmons, "Where is the cloud? geography, economics, environment, and jurisdiction in cloud computing," *First Monday*, vol. 14, no. 5, 2009.

[29] R. Clarke, "Computing clouds on the horizon? benefits and risks from the user's perspective," *23rd Bled eConference*, 2010.

[30] N. Sultan, "Cloud computing for education: A new dawn?," *International Journal of Information Management*, vol. 30, no. 2, pp. 109–116, 2010.

[31] S. Pearson, "Taking account of privacy when designing cloud computing services," in *Software Engineering Challenges of Cloud Computing, 2009. CLOUD'09. ICSE Workshop on*, pp. 44–52, IEEE, 2009.

[32] E. . Young, "Cloud computing issues and impacts." `http://www.ey.com/`, August 2012.

[33] L. Herbert and J. Erickson, "The roi of software-as-a-service," *White Paper*, 2009.

[34] D. Chappell, "Windows azure and isvs," tech. rep., Technical report, Microsoft: http://www. microsoft. com/windowsazure/whitepapers, 2009.

[35] E. Kotsovinos, "Virtualization: Blessing or curse?," *Queue*, vol. 8, no. 11, p. 40, 2010.

[36] B. A. Aubert, M. Patry, and S. Rivard, "A framework for information technology outsourcing risk management," *ACM SIGMIS Database*, vol. 36, no. 4, pp. 9–28, 2005.

[37] J. O. Fito and J. Guitart, "Business-driven management of infrastructure-level risks in cloud providers," *Future Generation Computer Systems*, 2012.

[38] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A berkeley view of cloud computing," *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*, vol. 28, 2009.

[39] K. Sripanidkulchai, S. Sahu, Y. Ruan, A. Shaikh, and C. Dorai, "Are clouds ready for large distributed applications?," *ACM SIGOPS Operating Systems Review*, vol. 44, no. 2, pp. 18–23, 2010.

[40] D. Durkee, "Why cloud computing will never be free," *Queue*, vol. 8, no. 4, p. 20, 2010.

[41] M. Lacity, L. Willcocks, and D. F. Feeny, "The value of selective it sourcing," *Sloan Man*, 2012.

[42] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*, pp. 109–116, IEEE, 2009.

[43] S. Mansfield-Devine, "Danger in the clouds," *Network Security*, vol. 2008, no. 12, pp. 9–11, 2008.

[44] S. B. Chebrolu, V. Bansal, and P. Telang, "Top 10 cloud risks that will keep you awake at night," *CSICO, available at: https://www. owasp. org/images/4/47/Cloud-Top10-Security-Risks. pdf.*

[45] M. Dalheimer and F.-J. Pfreundt, "Genlm: license management for grid and cloud computing environments," in *Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on*, pp. 132–139, IEEE, 2009.

[46] B. Grobauer and T. Schreck, "Towards incident handling in the cloud: challenges and approaches," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, pp. 77–86, ACM, 2010.

[47] Y. Mei, L. Liu, X. Pu, and S. Sivathanu, "Performance measurements and analysis of network i/o applications in virtualized cloud," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pp. 59–66, IEEE, 2010.

[48] E. Network and I. S. Agency, "Cloud computing information assurance framework," tech. rep., December 2009.

[49] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 199–212, ACM, 2009.

[50] P. C. Palvia, "A dialectic view of information systems outsourcing: pros and cons," *Information & Management*, vol. 29, no. 5, pp. 265–275, 1995.

[51] M. Creeger, "Cto roundtable: cloud computing.," *Commun. ACM*, vol. 52, no. 8, pp. 50–56, 2009.

[52] B. A. Aubert, M. Patry, and S. Rivard, "Assessing the risk of it outsourcing," in *System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conference on*, vol. 6, pp. 685–692, IEEE, 1998.

[53] E. Network and I. S. Agency, "Benefits, risks and recommendations for information security," tech. rep., November 2009.

[54] A. Khosravani, B. Nicholson, and T. Wood-Harper, "A case study analysis of risk, trust and control in cloud computing," in *Science and Information Conference (SAI), 2013*, pp. 879–887, 2013.

[55] A. Khajeh-Hosseini, I. Sommerville, and I. Sriram, "Research challenges for enterprise cloud computing," *arXiv preprint arXiv:1001.3257*, 2010.

[56] J. Huang, H. Yang, L. Xu, B. Xu, and H. Zhang, "Supporting contextaware service evolution with a process management requirements model," in *Service-Oriented Computing and Applications (SOCA), 2011 IEEE International Conference on*, pp. 1–8, IEEE, 2011.

[57] S. Zardari and R. Bahsoon, "Cloud adoption: a goal-oriented requirements engineering approach," in *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing*, pp. 29–35, ACM, 2011.

[58] J. Samad, S. Loke, and K. Reed, "Quantitative risk analysis for mobile cloud computing: A preliminary approach and a health application case study," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on*, pp. 1378–1385, 2013.

[59] N. Nahar, N. Huda, and J. Tepandi, "Critical risk factors in business model and is innovations of a cloud-based gaming company: Case evidence from scandinavia," in *Technology Management for Emerging Technologies (PICMET), 2012 Proceedings of PICMET '12:*, pp. 3674–3680, 2012.

[60] V. Kundra, "Federal cloud computing strategy," 2011.

[61] Cloud Computing Use Case Discussion Group, "Cloud computing use case white paper." `http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf`, July 2010.

Declaration

I hereby declare that the work presented in this thesis is entirely my own and that I did not use any other sources and references than the listed ones. I have marked all direct or indirect statements from other sources contained therein as quotations. Neither this work nor significant parts of it were part of another examination procedure. I have not published this work in whole or in part before. The electronic copy is consistent with all submitted copies.

Ort, Datum, Unterschift