An Investigation and Evaluation of Risk Assessment Methods in Information systems

Master of Science Thesis at
Computer Science and Engineering Department

By Feiquan Chen

Chalmers University of Technology
Department of Computer Science and Engineering
Göteborg, Sweden, 2015

An Investigation and Evaluation of Risk Assessment Methods (for Security Metrication)

Feiquan Chen

Examiner and Supervisor: Erland Jonsson

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

[Cover:
an explanatory caption for the (possible) cover picture
with page reference to detailed information in this essay.]

Department of Computer Science and Engineering
Göteborg, Sweden April 2015

Table of Contents

Figures and Tables

Acronyms List

AHP: Analytical Hierarchy Process
ALARP: As Low As Reasonably Practicable
ALE: Annualized Loss Expectancy
CCA: Cause-Consequence Analysis
COBRA: Consultative, Objective and Bi-functional Risk Analysis
CORA: Cost-of-Risk Analysis
COSO-ERM: Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management
ETA: Event Trees Analysis
FMECA: Failure Modes and Effects and Criticality Analysis
FRAP: Facilitated Risk Analysis Process
FTA: Fault Trees Analysis
IA: Information Assurance
ISMS: Information security management systems
ISO 27k: ISO 27000 (standards family)
MCDM: Multi-Criteria Decision Making
MCS: Minimal Cut Sets
OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation
PHA: Preliminary Hazard Analysis
PRA: Probabilistic Risk Assessment
RA: Risk Assessment
RPN: Risk Priority Number
SC: Security Category
SOL: Single Occurrence Losses

Acknowledgements

In the beginning of this thesis, I would like to pay my tribute to some people regarding to my thesis work.

First, I would like to express my sincerest appreciation to my supervisor and examiner Professor Erland Jonsson. He enlightened me with the initial thesis idea. And he has provided excellent guidance, brilliant advices, encouragement and availability during the whole thesis work period. I could not have accomplished this far without his help.

In addition, I would like to give my special thanks to my study counselor Elisabeth Andersson, for her generous help and advices regarding my thesis working conditions.

Finally I would like to show my deepest gratitude, as always, to my families and friends, for their selfless love and unconditional support.

Abstract

As technology develops and information society becomes more and more popular, information systems are involved in almost every aspect of people's life. One recent example is the uprising concept "Internet of things" that almost tries to solve everything within network and technology. With the convenience and benefits technology brings to us, risks also follow and threaten the environment we are enjoying. Wikileaks, NSA and Snowden, etc, those big dramas should make us more alert of those security issues and risks that we might encounter with information systems. In order to foresee the potential risks, predict the consequences and prepare the possible countermeasures, an exhaustive review into the risk assessment mechanisms we have today is needed. There are mainly three existing risk assessment methods: quantitative approach, qualitative approach and combined approach. This thesis makes a survey of the existing risk assessment methods (8 management tools, 2 technical tools, and 9 basic methods). It performs a comprehensive analysis and comparison between the different approaches, this involve reconstructing and grouping the surveyed methods according to their important factors, processing methods, and application environment. The weaknesses and benefits of the surveyed methods are discussed, and a risk assessment classification framework is proposed, dealing with risk assessment decision making or other related scenarios. Further, a systematic method is presented as an elaborate solution in the risk assessment field. Finally, the result of the study is considered in the broad picture of the risk assessment process design and implementation.

1. Introduction

1.1. Information security

Information security is to maintain the information's confidentiality, integrity and availability. The concept developed from earlier stages of Communication security, Computer security and Information security to nowadays Information Assurance (IA) [9]. According to IA, security is not only a status but a continuous process, including detection, response, protection, and recovery, as well as security management, education/training, legal support etc. The term information system refers to the (computer) system composed of equipment and facilities to accomplish data gathering, storage, transfer and application, etc. The purpose of security in information systems is to maintain the security and safety of information during data processing and other related system activities.

Risk exists in every process and every stage of an information systems' security activities. The process of studying information systems' risks is to use various methods and procedures from the risk management field, systematically analyze threats and vulnerabilities of the network and information systems, evaluate the damage level and propose prevention methods and countermeasures to protect the system from unexpected security incidents, in order to control the risk to an acceptable level. There are five major risks in the information systems that need to be assessed: organizational risk, infrastructure risk, definitional uncertainty, competitive response, technical uncertainty [7]. They are usually analyzed at different levels according to the organization's activities. One example can be seen in chapter 6.

1.2. What is Risk

There are many definitions of risks. According to Loudon and Loudon (1991) risk is taken to be a negative outcome that has a known or estimated probability of occurrence based on experience or some theory [11]. A formal expression, risk indicates the potential result of the security issues's probability and consequences. Symbolically we can put
Risk = f (probability, consequences). There are some similar concepts that might be confused with risks. In [4], the author explains the distinction between risk and uncertainty, risk = uncertainty + damage. For the distinction between risk and hazard, risk = hazard/safeguards. In the following chapters some extended definitions of risks will be mentioned with specific risk assessment approaches.

1.3. Why risk assessment

For information system security, we have to introduce risk management to the system as the key point of balancing the operational and economic costs of measurement to protect the IT systems and data. Through risk assessment of the system, we can be clearer about the system's security requirement and obtain a controllable, dependable and efficient security environment. After risk assessment we should be able to (a) identify the main security risks of information systems to help choose the right strategy to avoid or lower risks (b) understand the security status of the system to assure security requirement (c) build information security systems with a clearer goal, such as guidance to technical issues such as firewall deployment, IDS and IPS, etc, as well as management issues such as security management, education, and training.

Risk management includes three processes: risk assessment, risk mitigation, risk evaluation and assessment [3]. Risk assessment is the key part of risk management, it offers comprehensive procedures to identify the consequence and probabilities of the risk, and providing support for future decisions when dealing with the risk [1].

In ISO 31010 [1] the risk assessment process is divided into three stages, risk identification, risk analysis and risk evaluation. Risk identification is to identify possible situations that might cause a shift of the final goal. The cause, consequences, environment and related issues of the risks should be identified. Supporting technologies such as brainstorming, and Delphi methodology [12] can be used to improve the identification process. Risk analysis is to help the user fully understand the risk as it provides an input source for risk assessment, develops risk priority and acceptance level, and uses results for the further activities. There are mainly three types of risk used in risk analysis, qualitative, semi - quantitative or quantitative [1]. They will be briefly introduced in the next paragraphs and more discussion follows in the following chapters. A risk evaluation will finally decide the risk consequences and provide a basis for introducing countermeasures.

> - For Qualitative analysis the risk level is usually described in words or scales. It is normally based on previous survey records, employees' experiences, and experts opinions. The data is gathered from surgery or interview around the organization, then use the data to analyze the threats, weakness and control aspects towards the organization to quantify the existing risks. In today's complicated risk circumstances quantitative methods may not be so effective to simulate all the possibilities, thus introducing qualitative methods might help with the goal [6]. Qualitative methods are useful in situations when the analyzer did not have enough information or do not have qualified conditions to apply mathematic and statistic methods to the risk model [6]. It

can identify the risk in high, middle, low level without drawn into analysis of different figures of the organization’s operational data. Also, it makes it easier for professional employers without much risk knowledge background to participate in the analysis process. On the negative side, qualitative analysis usually lacks the support of figures. It mainly relies on subjective judgment, i.e. on like analyzer’s experience and can not offer very objective decisions.

- Quantitative analysis uses mathematical and statistic methods to convert the risk information gathered at previous stages into a measureable value. It supports the risk analysis result with quantitative value and standard, so that the objective result (compared to qualitative method) is more dependable and easy to accept and understand. But the process is usually very complicated and time consuming. There are various methods and standards to gather data and to calculate the quantitative value of risks, and they usually have very high requirement on the accuracy and integrity of the data that being collected for the analysis. So usually it is quite impossible to quantify the whole process of the risk assessment.

- Semi-quantitative risk analysis is used where one is attempting to optimize the allocation of available resources, in order to minimize the impact of risks towards one organization. It offers the advantage of being able to evaluate a larger number of risk issues than quantitative risk assessment because a full mathematical model is not necessary [27]. Semi-quantitative risk analysis uses numerical rating scales to represent risks consequence and probability, and make the overall risk assessment using formulas [1]. Since these numbers are indicative and usually the prequisite of the quantitative analysis, it is not an accurate representation of risk. Users should be careful of using semi-quantitative analysis because semi-quantitative analysis may lead to various inconsistencies: the numbers chosen may not correctly distinguish different risks, especially when the consequences or likelihood are extreme [10].

The rest of this paper is organized as follows. In chapter 2, the research method and research goal is presented; the survey process is described to ensure this work is done in a scientific and systematic way. In chapter 3, risk assessment key concepts are studied, the scope of this study is identified, and it provides theory support for the following chapters. In chapter 4, survey results of various existing RA methodologies are illustrated; the collected data are the input to the comparison and framework in the next chapter. In chapter 5, a comparison between the quantitative and qualitative approach is done, different RA methodologies are evaluated based on previous studies, and a decision framework to help the user choose the right method is developed. In chapter 6, a self-developed RA process mainly based on previous methodology is introduced to show how flexible and efficient usage of existing RA methods could be accomplished. Finally, a conclusion is given based on the study I have done.

2. Research Methodology

This chapter discusses the research purpose of the work, shows the review methodology used in the study and formulates the problem to be studied. The papers that have been reviewed are summarized in the end of the chapter.

2.1. Research Goals

The main goal of the research is to find an efficient and applicable way for assessing risks in information systems, considering that there already exist many methods that do the work. It would be accomplished by following the steps (sub-goals):

- To perform a comprehensive analysis of the risk assessment methods used in the selected papers
- To suggest a risk assessment classification framework for the methods used with respect to a selected set of parameters. Both quantitative and qualitative methods will be investigated.
- To make an evaluation and comparison between these methods
- To draw tangible conclusions on the pros and cons of the different methods
- To suggest possible improvements and/or new methods that would bring some further benefits to the area

2.2. Literature Review

A literature review is an objective, thorough summary and critical analysis of the relevant available literature on the topic being studied [1]. A successful literature review helps to catch up with the state-of-art progress in the field, support the author's credentials and build up a good theory base for further work or idea development. It can also help avoid repeated work and reveal the significance and potential of the ongoing work. In this thesis, the literature review will help to identify the main methods used in risk assessment of information systems. Based on the evaluation of the reviewer the further content of the studies will be decided.

The literature review process that this thesis is going to follow, is according to Rot [2]. It is made in five steps: problem formulation, data collection, data evaluation, analysis and interpretation, public presentation.

2.2.1. Problem formulation and search criteria

To start with the problems, research questions will be raised according to the goal this thesis wants to achieve. The main question to begin with is which are the existing risk assessment methods and how they implemented in practical assessment?

As further work continues, more detailed questions will be raised to assist the research:

- How should qualitative and quantitative methods be categorized and what are their benefits and weakness?
- What is the process and data flow of each assessed method?
- How do these methods contribute to security metrics in the whole picture?

Based on the goal and questions that have been raised, the search criteria will be clarified to help filter the articles. The inclusive criteria help include the articles for further review, and the exclusive criteria help exclude the articles that have been selected before:

- Inclusive criteria
    - Insight analysis and practical methodology of risk assessment of information systems, including qualitative and quantitative methods
    - Classic papers that are not limited to information systems' risk assessment but concentrate on more general and basic risk assessment methods
    - The newest version of the research material and standard documents in the field, if there exist several versions
    - Articles that are highly cited, well elaborated, clearly organized, and with firm and credible conclusions
- Exclusive criteria
    - Unrelated to information system's risk assessment or particularly focused on other specific fields that require strong background
    - Repeated or overlapping studies or data from the same field or the same methodology
    - Ambiguous and insufficient arguments of research and studies
    - Ambiguous or questionable conclusions of the studies
    - Old versions or under-development versions of the same topic

2.2.2. Search Strategy

In order to collect sufficient and reliable data, we need to clarify our search strategy and selection process, based on the search criteria stated previously. It begins with online searching of related papers from academic databases.

Most online search will be done in Google Scholar, Microsoft Academic Search and Chalmers Library, the most common academic database used in this research are such as ACM digital library, Scopus, IEEE Xplore, Web of science, etc. The keywords used for searching are: risk assessment, information systems, qualitative, quantitative, computer engineering, security, risk analysis, risk management. During the search different combinations of these words are used to fetch the papers that fits for the research criteria and goals.

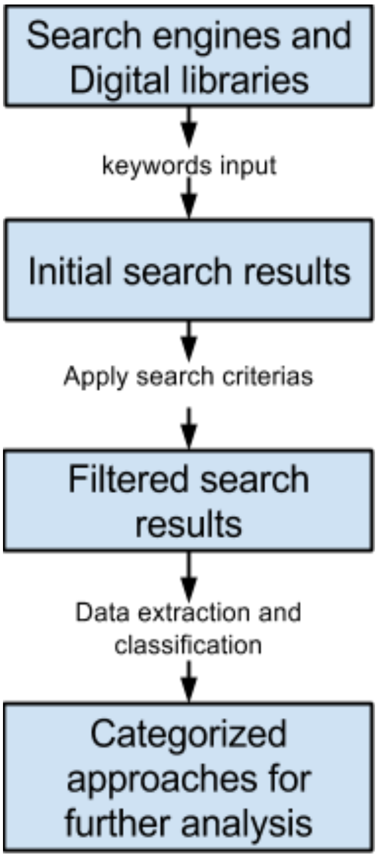

Search engines and Digital libraries
keywords input
Initial search results
Apply search criterias
Filtered search results
Data extraction and classification
Categorized approaches for further analysis

Figure 1. Search strategy

As showed in Figure 1, by typing the keywords into the search engine and academic database, a large number of papers that fits to previously defined requirements are showed. Applying the search criteria to these results leads to a reduced number of papers. In order to achieve an up to date survey result, the publication year and citation number are also two import factors to consider. For similar study with equal citation number, this study will refer to the newer research. There are also some classical papers with high reputations that appear in the reference list. The selected papers are categorized into different area for comparison and research purpose, which are Cyber risks trend, Independent Developed method, Cloud computing risks, Risk assessment guidance, PCI-DSS risk assessment, Risk assessment in E-commence, Risk assessment standards, Risk methods comparison, Quantitative methods, Qualitative methods, Semi - quantitative methods, Technical methods, Fuzzy theory, Bayes theory, Attack graph, and Related books respectively.

3. Risk assessment key concepts and scope

After selecting and going through all the materials, a literature review method will be applied to extract basic definitions and common criteria from the selected papers, so as to carry out the later parts of work. Following many risk management standards, such as ISO 27005 and ISO 31010, this thesis work regarding risk assessment mainly focuses on three parts: risk identification, risk analysis, risk evaluation. The RA process is not an isolated procedure but dependent on the context of the risk management process, something that requires pre-analysis, post-countermeasures, and coordination, monitor, feedback continually. The risk assessment structure and its relationship with risk management is shown in figure 2 [3].

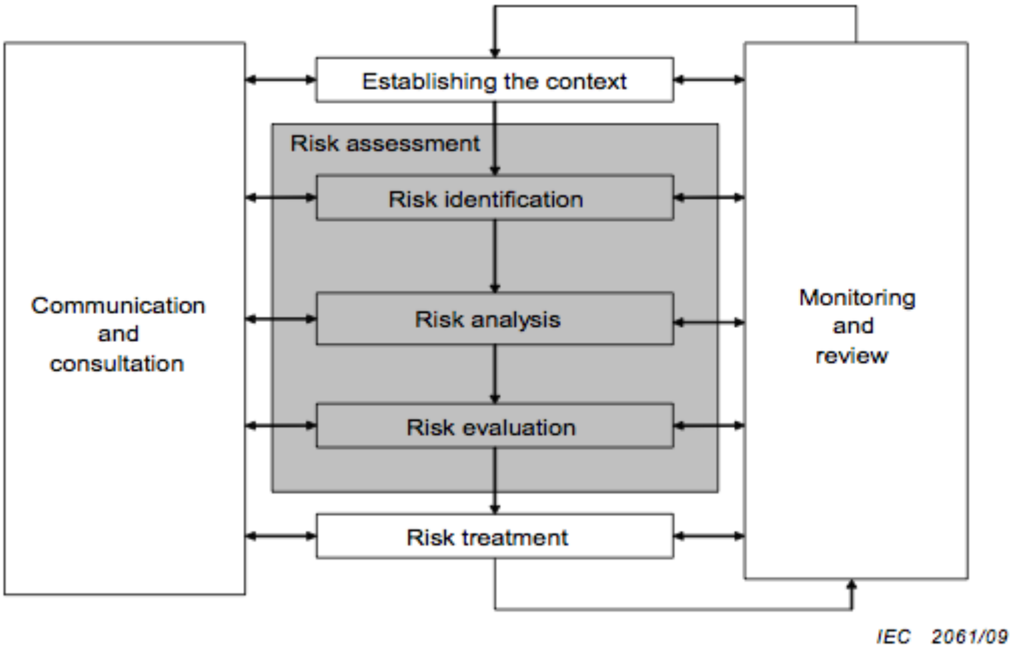


Figure 2. Risk assessment and the relation with risk management process **[1]**

Key concepts and data extracted from large number of papers will be shown in the following sections.

3.1. Risk identification

Risk identification is the process of finding, recognizing and recording risks [3]. According to [13], risk can be described as a function of the three variables threats, vulnerabilities and asset value. The external influence is threat, and internal influence is vulnerabilities, they act as input and source of the security incidents. The final consequence also depends on the asset value and environments. So these three attributes will be used as the basic input for a function that assesses risks:

$$R= f (a, t, v)$$

In the formula 'a' represents the assets value, 't' represents the likelihood that the threat will occur and 'v' represents the number of the vulnerabilities a system contains. There are other ways of interpreting the concept of risks. For example in [14], the authors proposed that risk is the combined effect of asset, threat type, threat source, vulnerability and countermeasure. Since most interpretations are expanded version of the basic three elements of risks, this thesis will use the basic triplet to evaluate risk. An information systems security risk assessment model is showed in Figure 3.

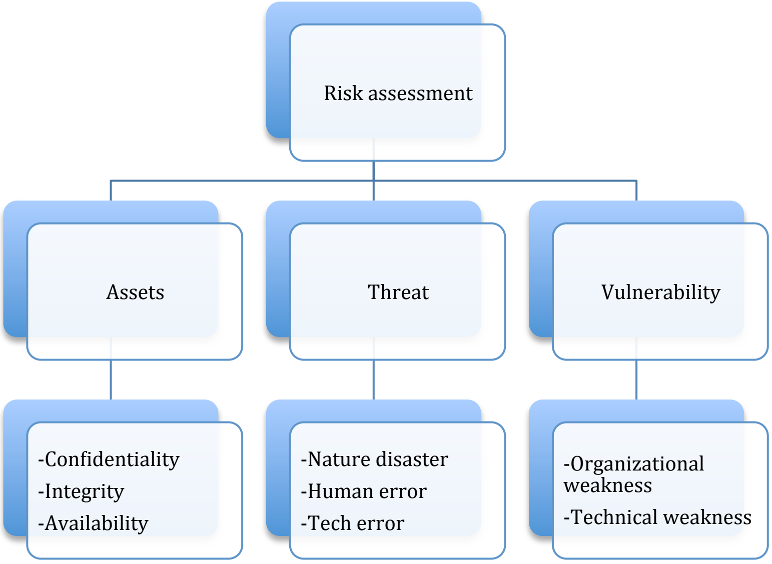


Figure 3. Information systems security risk assessment model

3.1.1. Assets

In information systems, the assets value is the worth of property for the organization, which is in danger. We will only consider the assets that have connections to information systems in this thesis. The assets can exist in different forms, tangible or intangible, hardware or software, service or infrastructure, etc. There are three parts of information assets that we need to consider, the information itself, the facilities that deals with information, and the people deal with the information. The facility's risk assessment is already regulated in the facility purchase stage, which the facility's risk will depend on the facility's performance under user's requirement. And the human resource is in general the organizational management field. Thus the information itself will be the core part to consider in assessing the assets of the information systems. Categorization of the assets in order to carry out a more efficient risk assessment is also important. According to [15], the assets can be categorized based on usage, e.g. information assets, physical assets, software assets, human assets, intangible assets, etc. FIPS PUB 199 [17] gives a concept of security categorization, the information assets can be valued based on three dimensions: confidentiality, integrity, and availability. Expressing the security category (SC) for information systems can be done as follows:

SC (information system) = {(confidentiality, *impact*), (integrity, *impact*), (availability, *impact*)}

The impact of each element is given as low, moderate, high or not applicable. This method gives an intuitive way to identify the information assets' security level.

Identification of the assets in risk assessment is a prior step to assessing the value. The important issue is to identify a large number of assets, and the correlation between assets. During the first round of assessing, it should be conducted as thoroughly as possible, in order to identify all the assets. Then the important assets and segments of the system can also be identified, in an assets table [16].

Evaluation of the assets is to be done after the identification of assets, in order to achieve a categorization of assets. The evaluation can be done in qualitative or quantitative way. The qualitative way is to list the importance of the assets, based on the assets' security level as determined by three aspects, confidentiality, integrity and availability, as previously discussed. Then a metric of the assets importance can be achieved [17]. The quantitative way for evaluating the assets is based on the actual environment and the value of the assets. A more detailed example will be discussed in Chapter 6.

3.1.2. Threats

Threats refer to those events that cause harm to information systems in general. More precisely, according to NISP SP900-30 [3], a threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. There are three aspects to consider in threat likelihood: threat-sources, potential vulnerabilities, and existing controls. To identify threat-sources, all potential threats towards the important assets should be recognized. Threat-sources can be categorized into environment factors or human factors. Environment factors are usually irresistible and consistent in certain background, such as earthquake or flood. User should always consider environment threats according to their operation environment even though it is difficult to avoid them. Meanwhile human factors are more of our concern because they are vagrant regarding to different people and different situations, and it is more difficult to predict human behavior than regular nature disasters. The existing form of a threat can be a direct or indirect attack against the systems, such as unauthorized modification, leaking, etc, that leads to violation of the confidentiality, integrity or availability of the system, or an unintentionally incident. In NISP SP800-30 [3], the human factors threats are listed as source, motivation, and threat actions. To quantify the likelihood of threats, three aspects should be considered:

1. Statistics of threats in previous security reports;
2. Collection of data in practical environment using intrusion detection tools, by checking the log files or other methods;
3. Reference of authoritative sources that have satisfies of the popular threats.

3.1.3. Vulnerabilities

A vulnerability refers to the openness of an information system to the threats. System vulnerabilities are usually exploited by the identified potential threats. In [16], vulnerability refers to the weakness that is related to the organizations' assets, sometimes that could cause an unexpected incident. In [3], vulnerability means flaw or weakness of the system's security flow, design and implementation that could lead to a security breach or violation of the security policy. Vulnerabilities can be divided into two categories. First is the vulnerability that affects to the asset itself, such as a technical issues, system breaches, etc. Second is the vulnerability that caused by insufficient organization management in a higher level [16]. Vulnerabilities and threats can be identified through documents audition, people's interview and questionnaires, on-site inspections, vulnerability scanner, etc [19].

3.2. Risk analysis

According to the ISO 27000 definition, risk analysis is the process of comprehending the nature of risk and to determine the level of risk [39]. From the definition we could find that the nature of risk is the cause and the source, then from the cause and the source we can identify and locate the risks. Different risks being identified in the RA process requires quantitative or qualitative methods to compare and decide the their priorities. Because not all risks will be considered. There are urgent ones or high danger ones, compares to not so urgent ones. This would lead to a priority table of different risks after analysis, and it would provide data bases for the next step risk evaluation and mitigation. As this part directly decide the risk values or levels, so it is the key part of risk assessment. A more detailed discussion about quantitative and qualitative risk methods will be presented in chapter 5 and 6.

3.3. Risk evaluation and mitigation

After the analysis of the risks, which usually in the form of qualified or quantified risk lists, the results should be compared with the given risk criteria, which is the reference for risk severity. The risk criteria can include cost-benefits, laws and regulations, economic and social environment, human factors, etc. With the comparison to a standard reference, it is easier for users to evaluate risks and take countermeasures under different circumstances. For taking actions against different levels of risk in various environments, there are four basic approaches [45]:

- Mitigate the risks, such as patch the system;
- Transfer the risks, such as outsource the unfamiliar operations to professionals;
- Avoid the risks, such as isolate internal network from outside network;
- Accept risks, if the potential risk consequences are acceptable under certain situation.

4. **Review of Risk assessment standards, tools and methodologies**

In this chapter commonly used risk assessment standards, tools and methodologies have been survived. RA standards provide a general guide line for risk assessment activities, while RA tools are systematic solutions and procedures that help conduct the risk assessment, some are developed by business organizations and requires royalties. RA methodologies are basically free and fundamental approaches to assess risks, some of them address a certain part of RA process and others cover the whole process. RA tools usually developed based on several RA methodologies.

After the input data of assets value, likelihood of threats and vulnerability of the system, under the guidance of industrial and academic standards, risk assessment tools and methodologies will be applied to process the data, evaluate risks and help decision making. These tools and methodologies have two basic approaches, quantitative and qualitative, some of them will use a mixed approach depending on the usage environment and process structure.

In this survey part key characteristics of each method are withdrew through analysis and parallel comparison, and data are collected for later constructing decision framework.

4.1. Standards

There are different standards and structures proposed to risk management and assessment. They have different emphasize and some old standards are now merged into new standards. Organizations should have chosen the standard that fits for them. The typical ones are ISO 31000, which some definitions are referred to in the beginning chapter 3; ISO 27001:2013 (previously known as BS 7799), ISO 27002:2013 (previously known as 17799), together with other support documents they formed ISO 27000 family that covers ISMS (information security management systems) definitions, requirements, measurements, guidance for implementation and management; And NIST 800 standards family, it is also widely used in the field of risk assessment, it is constantly updated for providing a management standards and guidance to secure and protect sensitive information.

The ISO 27k standards family originated from British standard BS 7799 (later with several updated versions and ISO 17799). The development process has included opinions from various fields including government, research organizations, industrial associations and international enterprises. And it continues to be updated and expanded to deal with the new trends in the fast developing technology fields. The ISO 27k standards have been adapted by many countries and the related business such as standards implementation and certification are operated all over the world. It is one of the most commonly recognized and accepted standards globally regarding to information security risk management. The reason is that they provide effective, full scale security risk management measures, and more importantly they offer motivations and goals to establish ISMS structure, which matches people's growing attention to information security management. Unlike other traditional approaches and standards that are based on technical understanding, the ISO 27k series gives a systematic, procedural and documentation framework for ISMS. It covers risk issues from organizational high level to a detailed operational and technical level. The technical emphasis is only a part of the procedure that enhances the overall security status of the structure. There are numbers of sub-standards under ISO 27k standards. The standards that are referenced in the following are:

ISO 27000:2014 - ISMS overviews and specialist vocabulary explanation
ISO 27001:2013 - ISMS requirements, performance and specifications
ISO 27002:2013 - ISMS control measures
ISO 27003:2010 - ISMS implementation guidance through cases
ISO 27004:2009 - Information security measurement and metrics for ISMS implementation and security evaluation
ISO 27005:2011 - Information security risk management process/methodology
ISO 27006:2011 - ISMS certification requirement for unit to provide ISMS certificate service

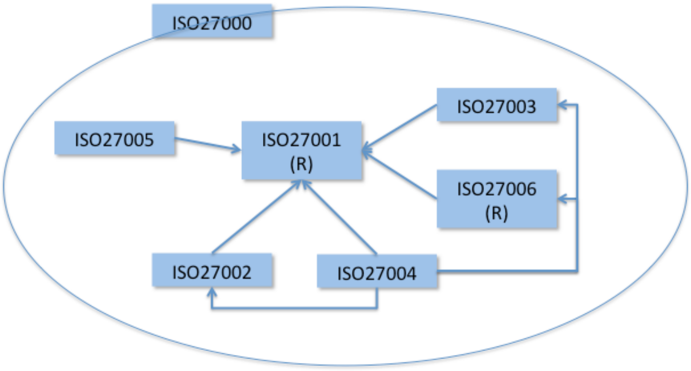


Figure 4. Inner-relations in ISO 27K Standards family

In Figure 4, R stands for requirement, while the rest are general guidelines. There are other supported standards in ISO 27K standards family, the introduction of which their relations can be found in the ISO 27000 document [39].

ISO 31000 is another popular standard in the risk management and assessment field that the thesis has referred to before. It provides principles, a framework and a process for managing risk, and it can be cooperate and be integrated with ISO 27001. ISO 31000 does not offer any specific advice about information security risk assessment and risk treatment. Therefore when solving information security problems, we need to look into other specific standards such as ISO 27005. However, ISO31000 can be a good supplement to provide a strategic framework for general risk management issues [40].

NIST SP 800 includes a series of practical guidance to information security technical and management issues, such as: SP 800-12 An introduction to Computer security - The NIST Handbook; SP 800-26: Security Self-Assessment Guide for Information Technology Systems; SP 800-30: Risk management Guide for information Technology systems; SP 800-34: Contingency Planning Guide for information Technology Systems, etc. They can be used as a reference and guidance book for risk assessment, and provide supplementary details to the ISO 27001 standard.

There are other standards that might be used in this thesis but not specially designed for information systems, so they will not specially be mentioned here. The detailed application of ISO 27K standards will be discussed in Chapter 6.

4.2. Tools

4.2.1. Management tools

a. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

OCTAVE is an approach for managing information security risks, developed by MIT and widely used around the world. Unlike other technology-oriented approaches, OCTAVE is more focused on strategic assessment/planning and organizational risk, and to achieve a balance of operational risk, security practice and technology. The three phases of OCTAVE are 1) build asset-based threat profiles, 2) identify infrastructure vulnerabilities, 3) develop security strategy and plans. The OCTAVE criteria are a set of principles, attributes, and outputs, so it can create various methods to apply to the actual usage environment of organizations. The OCTAVE Method is mainly for large organizations (more than 80 people), and OCTAVE-S is used for smaller organizations (20 - 80 people) with a reduced set of procedures [18].

b. Consultative, Objective and Bi-functional Risk Analysis (COBRA) [33]

COBRA includes a series of risk analysis, consulting and security evaluation tools. It is an expert-system-based risk assessment tool. It uses questionnaires to collect data, analyse, and assess the organization's risk in qualitative way. It contains three parts: question building, risk surveying, report generation. The new version is under re-development and enhancement now, that it will be possible to purchase once it is finished.

c. @RISK (with Monte-Carlo) [19]

@RISK is a quantitative tool for risk assessment based on Monte-Carlo simulation. It allows users to apply all kinds of probability distribution functions for building models. And for every incident's possible occurrence possibility and consequence, @RISK can assess the them and present the results in form of graphics or tables, so that the user can make the decision more intuitively under the risk environment. @RISK is usually work with Microsoft Excel environment.

d. CORAS [20] [22]

CORAS provides a tool supported framework for conducting efficient risk assessment of security critical systems. CORAS is a model based method and provides a customized language (usually UML) for risk modeling. The CORAS risk assessment methodology builds on HAZOP, FTA, FMECA, and provides support for integrity, availability, accountability, authenticity, and reliability of IT systems. There are 7 steps of CORAS risk analysis: introduction, high-level analysis, approval, risk identification workshop, risk estimation workshop, risk evaluation and risk treatment workshop.

e. Cost-of-Risk Analysis (CORA) [29]

The CORA risk model uses data collected about threats, functions and assets, and the vulnerabilities of the functions and assets to calculate the consequences, that is, the losses due to the occurrences of the threats. It is a methodology where the risk parameters are expressed quantitatively and where losses are expressed in quantitative monetary terms. CORA consist of two-step process: First it provides documents for user to collect and validate risk related parameters; Secondly CORA calculates SOL (single occurrence losses) and ALE (annualized loss expectancy) for each of the threats identified. It estimates a single loss value for a threat to an organization, and then multiplies this value by the frequency of the threat occurrence.

f. Facilitated Risk Analysis Process (FRAP) [34]

This qualitative method is mainly focused on the RA process with limited time and budget requirement, so it is usually faster and simpler compare to other methods. Four basic steps are conducted: Brainstorming to identify threats, assign impact of probability score to each threat, identify and assign controls/safeguards, and management summary. The method only filters and assesses the risk of activities that are most necessity. It didn't calculate the risk probability and ALE (annualized loss expectancy). Each member of the Risk assessment team needs to decide the importance of each risk based on his experience. Thus this method can control the assessment process using a relatively small process and improve the efficiency and lower the cost.

g. Committee of Sponsoring Organizations of the Treadway Commission Enterprise risk management (COSO-ERM)

COSO-ERM defines enterprise risk management as "...a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives [35]." It contains 8 related components, as showed in the one axes of the model figure 5, and 4 objectives. The objectives indicate the purpose of the activities, and components indicate what needs to be done. The third dimension shows different units in the enterprise. In order to assess the risk, the user can interpret from different angles or from a combination of all three dimensions. The downside is that the method relies on human decision, so the result might be limited to the ability and integrity of the decision group. Consequentially there is no absolute guarantee of the correctness of the result.

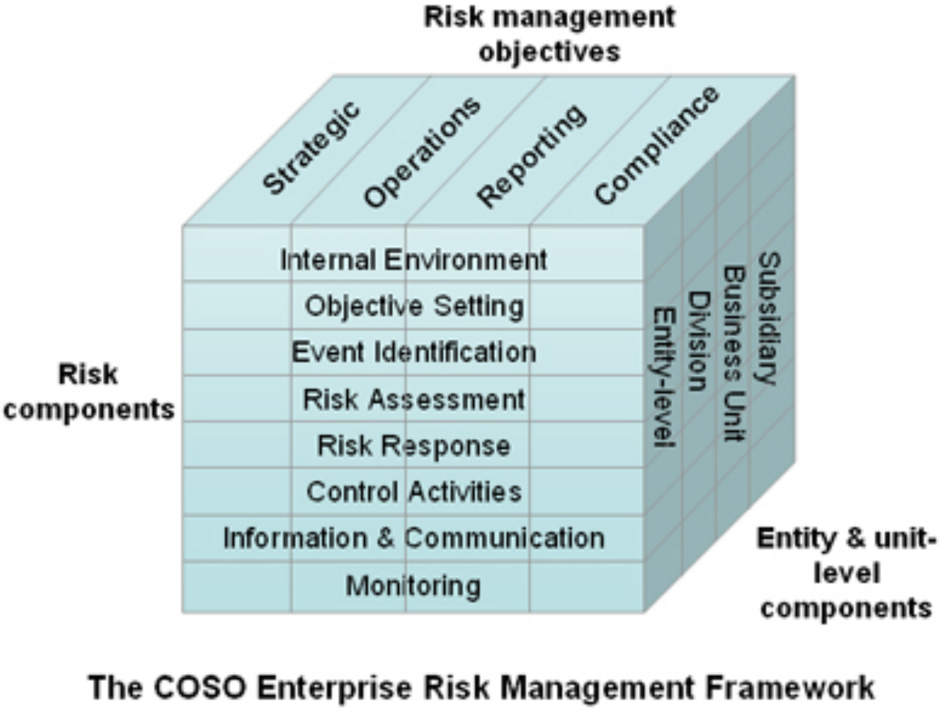


Figure 5. Coso - ERM Framework [36]

h. Risk Watch [37]

Risk Watch is a risk assessment tool that combines both quantitative and qualitative assessment approaches. It supports ISO 27k and other risk assessment standards and it can be used to analyse organizations, facilities, systems, applications or networks, in small or large scale. The tool contains 5 products that focus on different areas, out of which this thesis will only aim at the information system security part. Risk Watch has an advantages such as a friendly user interface, uses a predefined risk assessment models and an expert knowledge database so that the user can assess the risks and vulnerabilities efficiently. Further, it provides easy access to various platforms so as to improve the usability and corporation. It can also allow the user to customize assessment templates and processes according to their practical needs. It is very rare that risk assessment tools provide such function. The definition of risk in Risk Watch is to consider the aspects of assets, losses, threats, vulnerabilities and protection. The result of Risk Watch is to reach two goals, identify the risks under current situation, and find or recommend risk mitigation or reduction measures and prove that they are effective.

4.2.2. Technical tools

a. Vulnerability scanners

Vulnerability scanners are tools that assess the security of the networks or systems and are able to identify and report their vulnerabilities. They will scan networks, servers, firewalls, routers, applications, etc, in order to find the security breaches in the systems, and severity there. This is done from different levels of the system: network level assessment, operation system level assessment, database level assessment, and application level assessment. It should be done regularly so that the users can be updated about the potential risks. Typical vulnerability scanners are port scanners (Nmap, Nessus), Web application scanners, Host based scanners (Secpod Scanner), database scanners, etc.

b. Penetration testing

Penetration testing is a precautionary measurement to verify the harmful effects of a vulnerability of the system, so that the administrator could fix them before real attacks occur. It is usually conducted by carrying out a simulation of attacks that are similar to the reality but controllable and recoverable. People can use either a white box or a black box approach. In many cases penetration testing can be work together with vulnerability scanners. Vulnerability scanners are more efficient, but may cause false alarms and have problems to discover complicated security problems. Penetration testing on the other hand requires more time and resources investment, but is able to deal with more in-depth and logical breaches.

4.3. Methodologies

a. Hazop [21]

Hazards and Operability is a systematic method for detecting potential risks of a system that is usually carried out by a group of experts. The experts make an assessment of problems and risks through brainstorming and discussion, They analyze the cause, likelihood, possible consequences and their severity. Key words and key parameters will be used to analyze the abnormal behavior that is threatening the systems. Thus, the user can take countermeasures to control the risks. Hazop is a qualitative approach, and aimed at identifing problems without too much emphasis on solving them. The result of Hazop could be a threat list. Each threat will need a further assessment of the causes and consequences. The figure 6 introduces the operation flow of Hazop procedure.

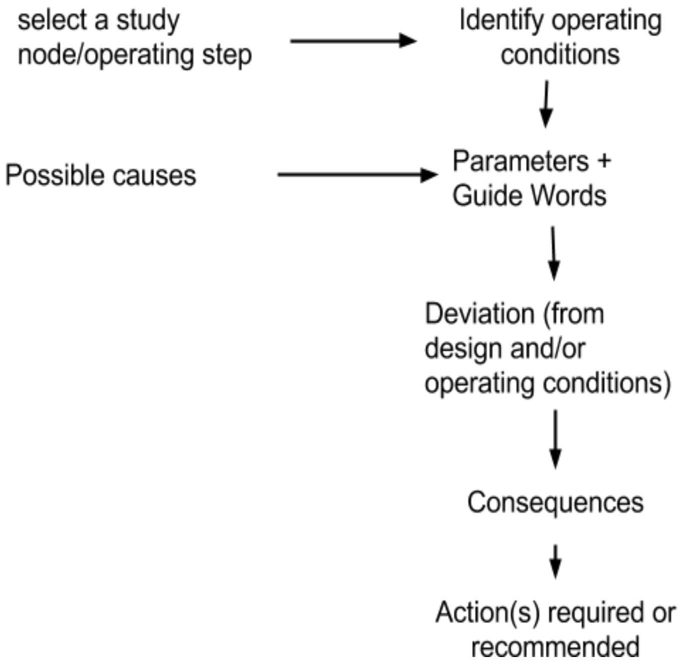

select a study node/operating step
Identify operating conditions
Possible causes
Parameters + Guide Words
Deviation (from design and/or operating conditions)
Consequences
Action(s) required or recommended

Figure 6. Hazop procedure operation flow

b. Probabilistic Risk Assessment (PRA) [23]

PRA is a model to analyze the frequency and consequences of not achieving a safe, stable end-state. [38] It combines both quantitative and qualitative methods for assessing the risks. PRA follows a series analysis steps:

-To identify events that could transfer potential hazards into real accident, record them as risk profiles.

-Evaluate the risk profiles with their roles in the system and their internal logic relations.

-Form a risk tree of the system, and assess the consequences and frequencies of risks.

-Use logical or mathematical approaches to get the final measure of the risk.

In the first stage of PRA, identification is carried out either by general engineering evaluation, based on previous experience and documenting history [25], or by a more formal approach such as Preliminary Hazard analysis and Failure modes and effects analysis and criticality analysis. Event trees and Fault trees are also important techniques that are used in this stage, and works as the bases of the PRA method.

c. Preliminary Hazard analysis (PHA) [26]

PHA is applied during the initiating stages of a project when the data and information is insufficient. A checklist study with consideration of event sequences that transforms hazards into an accident is conducted to identify the events or hazards. The effects of the events or hazards will be ranked according to the severity, and improvement will be made based on the ranking list.

d. Failure Modes and Effects and Criticality Analysis (FMECA) [23]

FMECA is composed by two parts: FMEA (Failure modes and effects analysis) and CA (Criticality Analysis). FMECA is an analytical and audition technique aiming at failures of the system and equipment. The first part, FMEA, is a method of exploring the failures modes of individual components of a system. In order to perform the FMEA process, you have to first understand the system, product and process. Then a worksheet will be set up for identify the failure modes of each components, based on five aspects: 1) how the component fail, 2) what is the cause of the failure, 3) what's the consequence of the failure, 4) how serious it is and 5) how the failure is detected. A countermeasure will be prepared to mitigate risks according to the worksheet analysis. This method can be time consuming and costly due to the large amount of data and information process. However it can improve reliability and quality, make it possible for earlier identification and elimination of the failure modes, and minimizes change costs. Once made it can be used as a valuable risk reference for the future operation. CA is an extended part of FMEA, through two additional steps. The first step determines and ranks the severity of the effect of the failure, estimates the likelihood of the occurrence of the failure, and how often a failure can be detected with the system's current security mechanism. Secondly a Risk Priority Number (RPN) will be calculated based on the previous analysis. We get RPN=(Severity)*(Probability)*(Detection). The higher the value is of RPN, the higher should the motivation be to adjust the failure modes.

e. Fault trees analysis (FTA)

Fault tree analysis is a graphical analysis technique from 1960s, which mainly is used for analysis of the reliability and security of complicated systems. It is a top-down approach. Through the analysis of the system's possible failure parts such as hardware, software, environment or human issues, we can draw an analysis tree graph that includes different combinations of the failures events and their probabilities.. The processes to performing FTA are:

1) Select a top event and analyze the related basic events, intermediate events and external event, define the system's boundary, and construct a fault tree,

2) Simplify the fault tree, identify Minimal Cut Sets (MCS). Minimal Cut Sets (MCS) refers to smallest sets (cannot be reduced any more) of the basic events in the graph that lead to the events.

3) Qualitative analysis of the fault tree,

4) (Or) Quantitative analysis of the fault tree (if needed),

5) Prepare reports and countermeasures.

f. Event tree analysis (ETA)

ETA is another graphical analysis technique that is used to define accident sequences caused by a given initiating event. It can quantify and qualify the possible outcome so as to help assess the system and help users make decisions. The analysis logic of ETA is opposite to that of FTA, as the analysis begins from the consequence of the given event. In every node of the event tree, the consequence can be success or fail. Based on expert experience and a large number of statistic studies, we get the probabilities of each possible result. Together with the events relations showed in the ETA tree graph, the probability of each possible path that represents a developing event can be calculated. Thus the quantified risk of the event is obtained.

g. Cause-Consequence Analysis (CCA)

CCA is a method that combines FTA and ETA. Thus it includes analysis of both causes and consequences, and a unity of induction and deduction. It can identify the events chain that could lead to unexpected consequences. From analyzing the probability of different events in the CCA graph, the probability of each possible consequence can be achieved. And the overall risk level can be identified with the consideration of different consequences and their probabilities.

h. Delphi

Delphi is a typical qualitative methods, that was invented to make use of experts experience while trying to reduce the outside interference and misleading information as much as possible. Therefore, it should be used when we have a complicated environment with a large amount of information with not so much adequate information, but with large uncertainty. It is characterized by anonymity, independence, and feedback. It is a group decision method that ensures that everyone could express their thoughts as free as they can. The process of the method would show as follows:

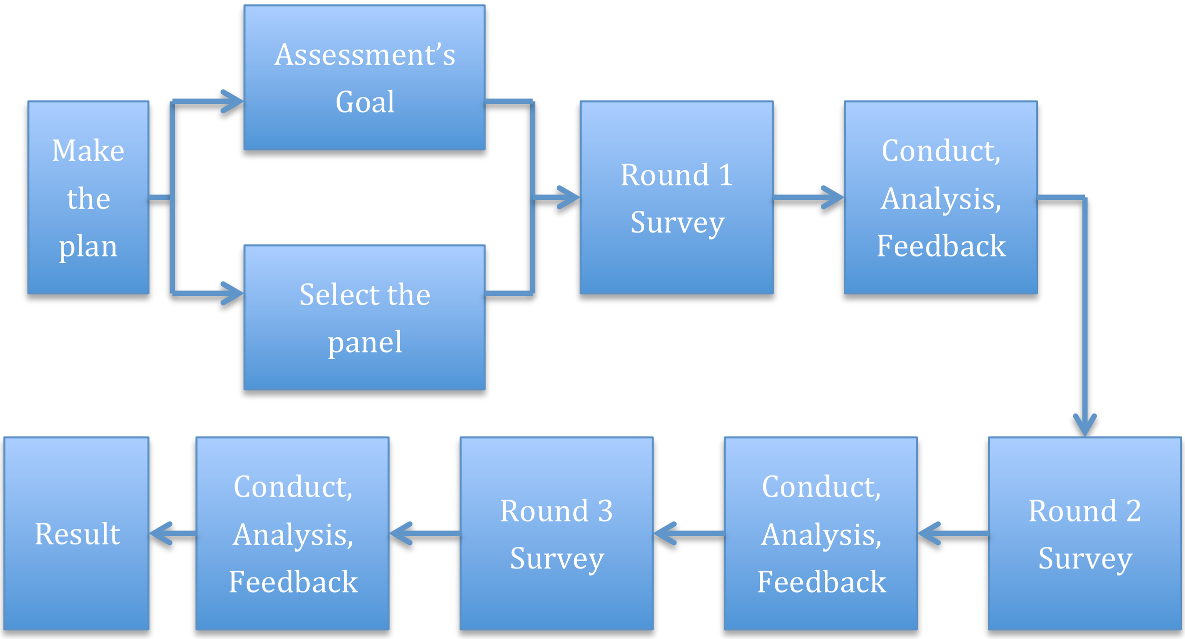


Figure 7. Delphi Methods Process [28]

i. Analytical Hierarchy Process (AHP)

AHP is a Multi-Criteria Decision Making (MCDM) method for risk assessment that combines both qualitative and quantitative approaches. It divides the decision process into layers by organizing and analyzing people's experience and objective thinking, so it suits for problems that are difficult to quantify in a direct way. The basic idea is to find the main factors from the problem analysis, construct these factors into hierarchy levels based on their relations. Then through pairwise comparison to identify the relative importance of these elements, and make the synthetically judgments of their priorities. The process of AHP includes 3 steps:

- Model the problem as a hierarchy: This would be a structure of three layers, the Goal layer, the Criterion layer to divide the goal and give more details, and the Alternatives layer to show the specific alternatives that influencing the goal.
- Evaluate the hierarchy tree by constructing a comparison matrix that compares the relative importance of different alternatives.
- Ordering and Consistency Checking: Rank the set of alternatives in order, first horizontal comparison in each layer to identify the relative importance, then vertical comparison to get the relative weight in the whole process for each element. Consistency checking will be implemented to identify the possible deviation that caused by the comparison matrix.

5. **Analysis of Methodologies**

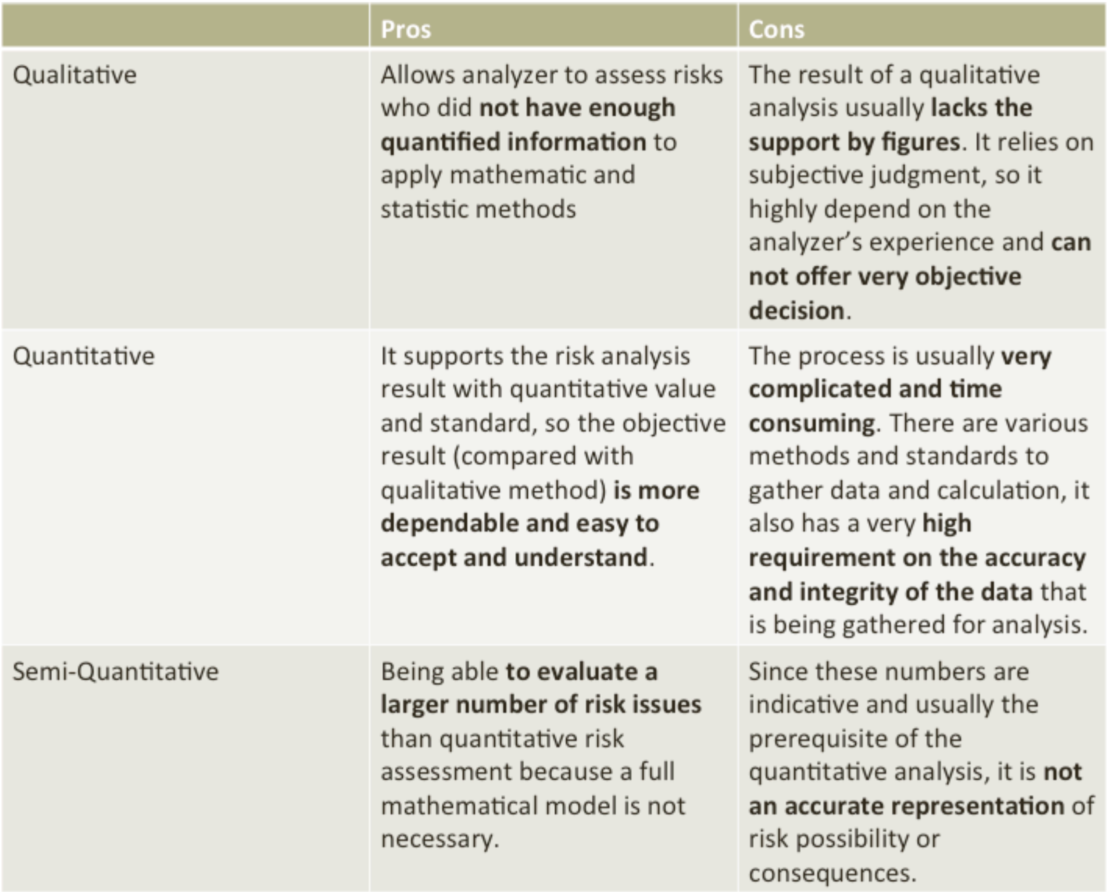
This chapter analyses the result collected from chapter 4, and compares different RA methodologies. Finally, it gives a decision framework to help users select the proper RA method according to their requirements.

5.1. Comparion of methods

Through the introduction in Chapter 4, we have a vision of current risk assessment methods in the information assessment process. We will need to categorize the methods to clarify the situation and show the pros and cons about different methods.

As stated before, the methods can be categorized into three types: qualitative, semi-qualitative and quantitative method. The pros and cons of each type have been analyzed in section 1, as summarized in Table 1.

Table 1. Comparison of different types of risk assessment approach



	Pros	Cons
Qualitative	Allows analyzer to assess risks who did **not have enough quantified information** to apply mathematic and statistic methods	The result of a qualitative analysis usually **lacks the support by figures**. It relies on subjective judgment, so it highly depend on the analyzer's experience and **can not offer very objective decision**.
Quantitative	It supports the risk analysis result with quantitative value and standard, so the objective result (compared with qualitative method) **is more dependable and easy to accept and understand**.	The process is usually **very complicated and time consuming**. There are various methods and standards to gather data and calculation, it also has a very **high requirement on the accuracy and integrity of the data** that is being gathered for analysis.
Semi-Quantitative	Being able **to evaluate a larger number of risk issues** than quantitative risk assessment because a full mathematical model is not necessary.	Since these numbers are indicative and usually the prerequisite of the quantitative analysis, it is **not an accurate representation** of risk possibility or consequences.

For each of the studied methods, a summary is made in the table below. It shows the characteristics as well as advantages and disadvantages for the methods:

Table 2. Qualitative methods

Method	Characteristics	Advantages	Disadvantages
Hazop	Identifies problems, and leave the solving part to the next step	Covers safety, operational aspects, human errors, process easy to learn and perform	Focuses on single events not all the possibilities, time consuming and expensive [30]
Delphi	Experts based assessment systems	Provides anonymity. Independence. Avoids objective judgment	Process complicated. And time is consuming
OCTAVE	Self-direction, Assessment based on single assets,	Only internal staff needed in the assessment, low cost, simple to use, [29]	Only a ranking of risks, indicating no relationship between different risks, not very accurate without mathematic approval
CORAS	Based on UML, different areas of experts brain-storm	Similar to OCTAVE	Similar to OCTAVE
ETA	Start from the initial events to find out the causes of different events routes	Able to find out different consequences of the failures and their probabilities	Can not analyze the parallel causes of consequences, not suitable for detailed analysis
CCA	Start from middle, forward using ETA, backward using FTA	Very flexible, able to cover most possibilities, easy to documentation and clear to show the cause-consequence relations	The graph can be complicated, similar to FTA

Table 3. Quantitative methods

Method	Characteristics	Advantages	Disadvantages
CORA	Single Occurrence Losses (SOL) or Annual Loss Expectancy (ALE) based	Little preparation and little information needed	External experts will be needed
FTA	From the original incident (top-down) to find out the composition of different dysfunctional and risks	Able to find out all possible causes of incidents and the ranking of different risks	Difficult to understand if a big faulty tree, including complicated logic relations, and need to know bottom events' probability

Table 4. Semi-Quantitative (combined) methods

Method	Characteristics	Advantages	Disadvantages
PRA	PRA provides insights into the strengths and weaknesses of the design and operation of IT information systems.	Can identify risks events and its causes, and the consequences and probabilities of the risk events	Requires the integrity and accurate of the collected data
AHP	Makes a Hierarchy of the system and quantifies the analysis to offer accurate support for decisions	Clear structure, good for decision making, able to assess the importance of different components under the whole system	Complicated mathematical calculation, time consuming
FMECA	Considers failure mode of every component to identify their relative importance	Improves reliability and quality, make earlier alarm, results can be reused in the future assessment	Time consuming and costly, hard to judge from a comprehensive view combining different aspects

5.2. Common Criteria in Decision Framework designing

Based on the analysis of different methodologies and previous studies [29] [31] [32], this thesis will propose a framework of strategy to select the most proper method in risk assessment for decision-making. The purpose is to make the end user more convenient to choose the right RA method based on their practical requirement and specification. Not all the methods that have been introduced are included in this selection framework. Only comprehensive, well documented methods are considered due to the practical usage environment and overlapping with basic and more advanced methods.

This thesis has selected several criteria commonly shared in different methods. They are comparable elements that show preference according to user's objective and purpose, which can help the user to determine the final choice. The criteria are divided into two different sections, cost/effect criteria and environment criteria.

5.2.1. The cost/effect criteria

The cost/effect criteria helps user to achieve good balance between budget and effect. In the decision making process, cost and effect is always a dilemma for the decision makers. In the ideal situation the user would prefer the solution to have best accuracy in risk result with lowest cost, but in reality usually this is the most challenging part. Some users might value the accuracy more than money if they could not afford the risks, and others would rather save some money if certain risks can be tolerated. The criteria is to help users choose the right method in their situation to find the balance point of cost and effect during the risk assessment process to reach the maximum economic benefit. During the risk assessment process, cost is affected by many factors. Four main sub-criteria are considered in this part. They are Quantitative or Qualitative, Time, Human factors, Usability.

1. Quantitative or Qualitative

It is hard to judge whether quantitative or qualitative method is better, we need different approaches in different situations. Under the same budget and time consideration, user would want the assessed result to be as accurate and convincing as possible. If we can have data to prove that, even though it might cost more time, and data itself in some situation is hard to collect or difficult to standardize, we would still consider that quantitative results would be more dependable and trustworthy than qualitative result. In the situation that a quantitative result is not the priority, we can lower the weight of this factor to minimize the influence of it in the decision process.

The score of the criteria are as follows, under the same budget consideration: a quantitative result is preferred over a qualitative result, and assigned with a higher value.

- If the method is based on quantitative or semi-quantitative approach, it values 2, The methods that combines quantitative and qualitative approaches will be consider score 2 because the final result is supported with quantitative data.
- If the method is based on qualitative approach, it values 1. As the qualitative result is less preferred than the quantitative result, so the value of qualitative method is lower than quantitative method.

2. Time

Time is a very valuable factor in the decision process. A time-consuming method might mean more complex and more accurate in risk assessment result, but will significantly cost more as the project lasts for longer time. The cost can be either in financial terms or opportunity terms. Different methodologies need different assessing time due to the fact that their process varies. This is because some methodologies are more complicated than others. They would cover different stages of system design/development, or need different values that require more time to fetch.

The score of the time criterion is as follows, i.e. under the same environment: less time consuming method is preferred to a more time consuming method, and assigned with a higher value.

- If the method is less time consuming, less preparation or not so many data need to be prepared, it values 3
- If the method is not so time consuming, with some data needed with not too much processing to prepare and collect, it values 2
- If the method is very time consuming, with a quite complicated process and lots of data/preparation involved, it values 1

3. Human factors

The human being is an important influence factor in the risk assessment process. The qualification and experience of the RA team members will lead to different quality of the result. For better result, we would want the assessment done by professionals. However not every company has such department or has enough talents for the job. Hiring external expertise would add to the budget, not only the service fee but also after-sale support cost, and cost for knowledge transfer and maintenance. Some methodologies need less professionals to be involved, or only internal people, such as OCTAVE. While other methodologies have requirement for external risk experts or certificated professionals, for example CORA. The less external people needed, we consider the method to be better, to save the cost and avoid the risk of leaking the risk information outside. But this is still a trade-off, if the user prefers a more professional and trustworthy, maybe standard (certified) result, it might be good to lower this criteria's weight and use qualified people from professional a RA consultant for the process.

The score of the criteria is as follows, i.e. means under the same environment: less external people involved method is preferred to a more complicated method that has to involve external professionals, and assigned with a higher value.

- If the method have flexible requirement on the staff that are involved in the risk assessment process, or easy to learn and implement without professional knowledge, it values 3
- If the method only requires few experts to help with the RA process, it values 2
- If the method requires or recommends experienced risk experts or certificated professionals to conduct the risk assessment, it values 1

4. Usability

The usability directly affects the implementation of the risk assessment method, and the future development or change of the project. Poor usability would mean that a method would be difficult to carry out and cost enormously, no matter how scientifically rigorous the method is. So we prefer a simpler method, within the methods that with same weight in usability criterion. There are several aspects to judge usability, like how the calculation is done for the method, if the mathematical formula is complicated or not. If the method is complex enough to require lots of extra training, or hard to maintain once the assessment is done, then it has poor usability. Also, some methods have just been developed still others are not used any more, so the usability is uncertain in this case. For methods with good usability, the company could save a lot of resources on the project. But if user is not planning to compromise on the process and result part, or if they value other factors more than usability, they might lower the weight of this criterion.

The score of the criteria are as follows, i.e. under same environment: a method with good usability is preferred than hard-to-use method, and assigned with higher value.

- If the method is simple in the assessment process, with no need of strict proof of the steps, and easy to maintain and no extra training needed to conduct the assessment, then we consider it as high usability, thus it values 3
- If the method is need certain proof over the assessment process, with the support of simple mathematical calculation, and some extra professional knowledge needed, we consider it as middle usability, thus it values 2

- If the method need complicated mathematical formulae or complex proved process, we consider it as low usability, thus it values 1

5.2.2. Environmental criteria

There are also some environmental factors that should be considered. These criteria have no direct connection to cost efficiency, but depend more on the risk assessment's requirement and objectives. By introducing environmental criteria, the user can be able to pick the ideal method not only based on economic issues, but also taking the practical environment into consideration. After all, companies and organizations have more responsibilities than just to consider economic aspects in risk assessment.

The environment criteria selected for the framework are:

1. Scope

The scope of risk assessment activities depends on the purpose and the capability of organization. A risk assessment method could only be focused on information security risks, or cover a greater range of areas. Choosing the risk assessment method with the appropriate scope could lead to more accurate result, provide redundancy and avoid waste. The criteria can be categorized into two different types: narrow scope or broad scope.

2. Flexibility

We can define the flexibility of risk assessment activities into two types: process flexibility and time flexibility. For process flexibility, some methods are designed to assess the risk of a single process in risk assessment project, while others are capable of analyzing more complicated system risks in an organizational perspective. We consider if the method could assess under complex environment and deal with different need, it is a flexible method. For time flexibility if the method could conduct the risk assessment just once and then start from the beginning again, or the method can work continuously and reuse the result iteratively. For time flexibility one example is that we might prefer methods that supports database analysis instead of simple spreadsheet so that the data in continuous RA operations can be used effectively. Thus in the criteria we categorize the methods to be flexible and non-flexible methods.

3. Standards Compliance: Some users might have requests for support from certain risk assessment standards document(s). This is due to risk assessment project purpose and requirement, usage environment or legal issues, regarding to the existing difference between different nation's law systems and interests. Besides from the standards introduced in section 4.1, there are other standards used in different countries such as AS/NZS ISO 31000

(Developed from AS/NZS 4360 from Australia and New Zealand), IT Baseline Protection catalogs (German Federal Office for Security in Information Technology), AN/CSAQ 850-97 (Canadian Standards Association Standard), and many more other documents by different standards organizations. This framework will only consider some most commonly used standards.

4. Purchase price: Some methodologies might require a certain amount of usage fees, depending on the developer or distributor of each method. The aspect listed here depends on the budget of the risk assessment project, and what level of support the user wants to get. If the project has a limited budget, then the user could skip costly method because there are many free methods on the market and they have been proved to be capable as well. The price criterion will categorize the methodologies into free methods and cost methods that user must pay for.

5.3. The decision framework for choosing risk assessment methods

As the criteria for the decision framework have now been decided, the methodologies introduced in section 4.2 and section 4.3 will be categorized in accordance. A framework will be developed to help the user choose which is the proper method under their requirement and situation.

For decision framework, we have two main parts to take into consideration: the cost/effect aspect and the environment aspect. The user should first decide how heavy they are willing to weigh each part. Sometimes a risk assessment project is under a tight budget so that economic aspect would be more critical; while in other situation it might be the environment that puts high requirements on the project. To help the user decide, the framework divided the decision process into two parts, the cost / effect aspect and the environmental aspect, and assigns a total weight to each parts, Wc and We, respectively.

5.3.1. The environmental criteria

The thesis has analysed each method based on the criteria provided in section 5.2, and assigned a value for each criterion individually. The detailed forms are provided separately in Appendix A. This will help the user quantifies their choices and increases the decision's visibility. For decision making, the decision framework proposes that the evaluation start out from the environmental aspect. This is because in practical usage the environment situation is usually not so easy to change or modify, while cost/effect aspect can be quite flexible and adjusted during the selection process. For each part of the analysis, we divided the methodologies into management tools, as they have a more complicated function and are more systematically developed, and basic risk assessment methodologies that usually serve as input to or source of the management methodologies. Some methodologies such as HAZOP are not very commonly used in information systems risk assessment, so they will be omitted in this part of the analysis.

For environmental criteria, the following Table 5 presents the relations and comparison between different RA management tools, and the Table 6 presents the relations and comparison between different RA methods. The explanation can be find in Appendix A.

Table 5. Decision table for RA tools based on environmental criteria

	Scope	Flexibility	Standards Compliance	Purchase price	Sum
OCTAVE	Narrow	Flexible	N/A	Free	
CORAS	Narrow	Flexible	ISO 31K, ISO 27K, AS/NZA 4360	Free	
CORA	Broad	Not flexible	N/A	Cost $7000 to $85000	
COBRA	Broad	Flexible	ISO 17799 → ISO 27K	Cost $895/$1995	
RISK Watch	Broad	Flexible	ISO 27K, ISO 32K, and other standards	Cost $15000	
FRAP	Narrow	Not flexible	ISO 17799/ISO 27K	Free	
COSO ERM	Broad	Not flexible	2010.A1, 2020.A1, 2210.A1	Cost	
@Risk	Broad	Flexible	N/A	Free (requires cost support software)	
Weight					

Table 6. Decision table for RA methods based on environmental criteria

	Scope	Flexibility	Standards Compliance	Purchase price	Sum
FTA	Broad	Flexible	BS7799/ISO27K	Free	
ETA	Broad	Flexible	IEC 61025	Free	
Delphi	Broad	Not flexible	N/A	Free	
AHP	Broad	Flexible	BS7799/ISO27K	Free	
FMECA	Broad	Not flexible	N/A	Free	
Weight					

The purpose of these two tables is to help the user decides about the right method that fits for their specific RA environmental situation. To quantify the result, the user first has to make a clear requirement list based on the environmental criteria listed above. Is the risk assessment only done with the IT security aspect, or do other fields also need to be considered? Do we need a method for assessing a simple target, or a complex system, or does the organization have both requirements? Are there any standards or local regulation we have to follow? How much can we afford to pay? There are more things the user needs to consider according to the criteria properties discussed above. If the user has decided what kind of environmental criteria that he need, then he will compare the list with the table above. First compare with the management tools table, then with the basic methodologies table. This is because management tools are prioritized since they represent the first level of the method that we are going to apply on the risk assessment. The basic methodologies, which serve as input or support is the second level of the method that we are going to use in the project.

To evaluate the methodologies, we first need to assign a weight to each row (W_{scope}, $W_{flexibility,}$, $W_{standards}$, W_{price}). This is the environmental criterion that is drawn from the analysis. Depending on the requirements for different risk assessment projects, the user needs to prioritize these environment criteria, and assign a percentage weight to each criterion. After the relative importance of each environment criteria is set, user will be able to pick the right method, according to their environment criteria list. For each environment criteria, if the method meets the requirement of the user, two points will be assigned to the criteria of the method, otherwise that part will be left with zero point. The score for the four environmental

criteria will be S_{scope}, $S_{flexibility}$, $S_{standards}$, S_{price}, respectively. For example, if a risk assessment project only needs to be done in a IT project, it only requires a narrow scope for the method, then OCTAVE, CORAS and FRAP would be suitable and will be assigned 2 points under the "scope" criteria. The user needs to compare his list with every criteria of every method, and get a table that makes him able to calculate the sum of each method.
For each method, we have

$$Sum_E = W_{scope} * S_{scope} + W_{flexibility} * S_{flexibility} + W_{standards} * S_{standards} + W_{price} * S_{price}$$

Where W is the weight for each criteria and S is the score for each criteria, as introduced in last paragraph. In a practical environment user might prefer some criteria than another by adding up to the weight. In this way we can get the total score for each method regarding their environment criteria, so that the user can judge which method is the best in a certain practical environment.

5.3.2. The cost/effect criteria

After summing up the environmental criteria, the user needs to assess the usability of the cost/effect criteria of each methodology. In Appendix A is given the detailed ranking for the methodologies as well as a rationale for the ranking. The analysis will be the same as the previous part, divided into management methodologies and basic methodologies.

Table 7. Decision table for RA tools based on cost/effect criteria

	Quantitative/Qualitative	Time	Human Factors	Usability	Sum
OCTAVE	1	1	3	3	
CORAS	1	2	3	3	
CORA	1	3	1	3	
COBRA	2	3	3	1	
RISK Watch	2	3	3	3	
FRAP	1	3	2	3	
COSO ERM	2	1	2	3	
@Risk	2	2	3	3	
Weight					

Table 8. Decision table for RA methods based on cost/effect criteria

	Quantitative/Qualitative	Time	Human factors	Usability	Sum
FTA	2	2	2	1	
ETA	2	2	3	2	
Delphi	1	1	2	3	
AHP	2	2	1	2	
FMECA	2	2	2	2	
Weight					

For the cost/effect criteria, the user wants to make the best economic outcome with his investment. In this way the thesis has proposed a way to rank the cost/effect criteria into 3 levels. To find the best result, which in an ideal situation should be the most accurate, easiest to use and cheapest, the user needs to evaluate the relative importance of the four cost/effect criteria, and assign a percentage weight to them. The assigned weight to each cost/effect criterion is W_{qua}, W_{time}, W_{human}, $W_{usability}$, respectively. This depends on the project's specific needs and the user's strategy. Then the total weight for each method could be calculated as:

$$Sum_{C/E} = W_{qua} * S_{qua} + W_{time} * S_{time} + W_{human} * S_{human +} W_{usability} * S_{usability}$$

In this equation, S_{qua} , S_{time} , S_{human}, $S_{usability}$ are showed in Fig 10 and Fig 11, for each analyzed RA tool and method. W_{qua}, W_{time}, W_{human}, $W_{usability}$ are introduced in the last paragraph. With this equation, user can quantify and identify the most efficient method for their individual risk assessment project.

5.3.3. Final decision for selecting the best methodology

With the relative priorities of each method known for environment and cost/effect criteria respectably, the user should decide which is more important, the environmental issue or economic issue, and how much weight he is willing to put on each part. Based on the situation, user can weigh the importance of cost/effect criteria and environment criteria by percentage, that is Wc and We respectively, and the final score for each method can be calculated:

$$Sum = W_e * Sum_E + W_c * S\,um_{C/E}$$

With this equation, the user will get a clear view of how close or how far each method is from the user's ideal solution. The method with the highest Sum would be the best methodology for the specific risk assessment project.

In normal situations, the user has a clear view of the risk assessment project and is able to map the detailed requirements into different weights of each criteria. He can choose the best RA method with the help of the decision framework introduced above. In some special situations that two or more RA tools that ends up with similar scores in the decision framework, which would make it difficult for the user to choose which one is the best for him. Table 9 shows the characteristics of each RA management tools. The user can use the table as a supplement tool to the decision framework for selection of the RA tools and methods, or filter for the proper tools in the beginning of the selection process under his specific requirement.

Table 9. Characteristics of the RA management tools

OCTAVE	A process-driven methodology to identify, prioritize and manage information security risks
CORAS	A practical framework for model-based security risk assessment
CORA	A risk management expert system for organizations, calculate ALE, Return on Investment, and forecasts the financial impact of risks
COBRA	Under re-development now
RISKWatch	Customize templates, easy access and full time monitor, friendly user interface
FRAP	Faster and simpler for software and computer company's risk assessment
COSO ERM	Principles-based , enterprise-wide approaches to risk management
@Risk	Monte-Carlo simulation, quantify multiple possible result for user to choose

There are other trends as combing different risk assessment methodologies together into IT system risk analysis, such CCA (Bow Tie analysis), HAZOP – FTA – ETA [49], AHP – Fuzzy theory [50]. The combined methods are based on the balance of the pros and cons of each method involved. In order to choose the best match for methods that would work together, the user can also use the decision framework presented in the this chapter. It clearly shows the benefits and weaknesses of each method. In the next part of the thesis I will introduce a new method based on the analysis in this chapter and the trend in industry.

6. Self-developed methodology

After selecting the right RA method for a project, the project team should be able to start with a risk assessment process. In reality, as we have observed before, no single method is perfect, and it may hard to find a perfect method for the risk assessment. Therefore, we need to tailor it or combine different methods to find the best solution. Nowadays, AI theory / machine learning / neural networks and fuzzy method are more involved in the RA process, and hybrid methods are more commonly used in practice. There exists a number of hybrid methods with various purpose and different emphasis. Some of the typical ones were introduced in chapter 5. This hybrid mode framework is able to provide a standard procedure to assess the organization’s risk that is compatible with generally accepted security standards. Here we will use the ISO 27k standards family as an example. The reason we choose the 27K standards family will be present in the next paragraph. Thus, this thesis will develop a new RA process based on the hybrid principle, trying to provide a good solution for information systems environment, and presenting a thinking process for developing a self tailored method.

6.1. Method foundation

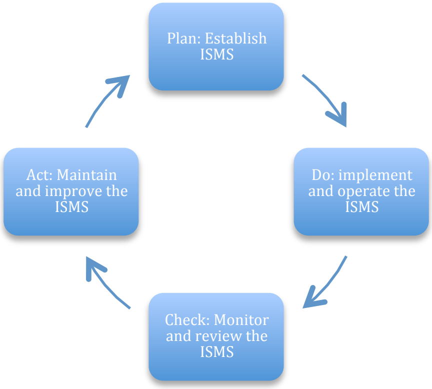
6.1.1. The concept of RAF

A Risk Assessment Framework (RAF) is a strategy to share and review the information flow regarding organizational risks. A good RAF should be easy for both professional and unprofessional staff to understand. It will not only focus on a single asset or system, but target the whole organization. The related environmental elements that are related to the organization’s operation should be considered, e.g. the organization’s goal, structure, documentation, etc. A good RAF can enable the organization to discover the potential risks, the relative level of risks, and help the organization to deal with the potential threats, making strategic development and financial plans, as well as cultivate a sustainable business culture. The existing RAFs that are widely used in the industry are ISO 27K, NIST, OCTAVE, etc, and an organization can apply them directly or modify them to create a new framework for their specific requirement.

6.1.2. Integration with 27k standards family

The self-developed RA method presented in the following will mainly integrated with ISO 27K standards family, but will also borrow some ideas from ISO 31000 and NIST 800-30.

These three standards families are introduced in section 4.1. The ISO 27K standards family follows the ISMS PDCA model with continuous improvement ability [39] [40].



Plan: Establish ISMS
Do: implement and operate the ISMS
Check: Monitor and review the ISMS
Act: Maintain and improve the ISMS

Figure 8. ISMS PDCA model defined in ISO 27000

As showed in Figure 8, ISMS continuously improves the RA performance and maintains the safety of the system. In the Planning phase, organizations identify assets and security requirements, assess information security risks and select risk controls. In the Do phase, the organization implements and operates the security policy defined in the last stage, in order to control unacceptable risks. In the Check phase, the organization assesses the effectiveness of the implementation, and reviews the performance. In the Act phase, the organization takes corrective actions and preventive measures to improve performance.

6.1.3. Key Problems to solve

The main tasks of risk assessment is to assess all kinds of risk that an organization may encounter, assess the probability and impact of risk, determine the resistance of risk for organization, decide the risk mitigation measures and corresponding reactions. There are several key questions to be considered:

1. What are the key assets that need to be protected? What is their direct use value and indirect use value?
2. What are the potential threats that these assets face? What is the source of the threats? What are the probabilities that these threats will actually take occur?
3. What are the vulnerabilities in the assets that could be used by the threats? And how easily can this happen?
4. Once the threat happens, what loss or negative effects may the organization face?
5. What security measures should the organization take to control and mitigate the risk to a accepted level?

6.2. The structure of the self-developed methodology

The method will be developed following the instructions of the ISO 27k standards family, and the key definitions will also be derived from the standards documents. In the following part will propose a detailed process and a model.

The purpose of this model is to target at all kinds of information related risks in the organization, so the ERM concept will be introduced, as the ERM Framework develops a portfolio view from three different levels: Entity level, Business level, Operational level, as shown in Fig. 4. According to COSO ERM model, for each level we consider eight risk components, which follow the PDCA model of the ISO standards as well, as showed in the process description in Figure 2. ISO 27005's instruction also stated that, "Risk assessment is often conducted in two (or more) iterations. First, a high level assessment is carried out to identify potentially high risks that warrant further assessment. The next iteration can involve further in-depth consideration of potentially high risks revealed in the initial iteration. Where this provides insufficient information to assess the risk then further detailed analyses are conducted, probably on parts of the total scope, and possibly using a different method [41]." To make the structure more flat and obvious, the process can be shown as in Figure 9.

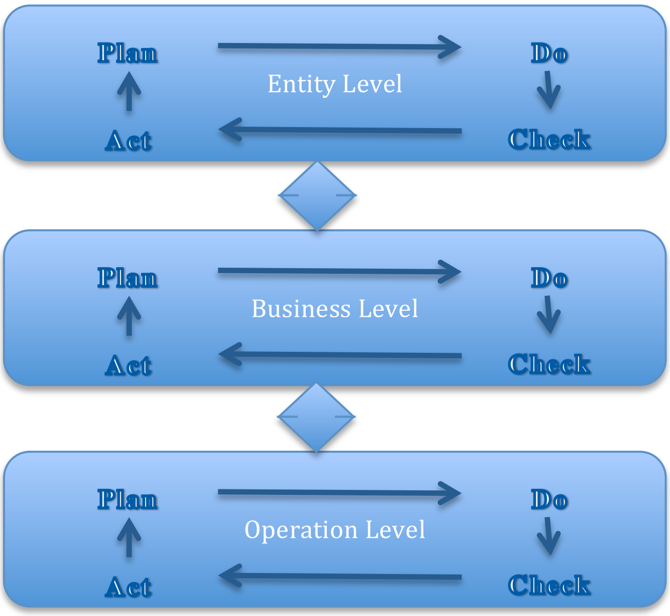


Figure 9. Data flow between different levels of IT systems in risk assessment activity

The data flow in between identifies information and guidance from the upper level to lower level, and the feedback information for continuous improvement from lower level to upper level. The Table 10 shows different roles of each level in the organization's risk assessment [41].

Table 10. Risk assessment in different level of the organization

	Risk emphasize	People involved	Data flow
Entity Level	From the organization point of view, based on organization policy, strategy and structure	Top Executives, Head of different Business Units	Function/Output: Strategically analysis and guidance of the organization risk assessment
Business Level	Target on Business process and project missions	Head of Business Units, Business analysts, Project Managers	Function/Output: Tactic analysis and specific risk assessment goals on business unit , coordinate policy and operation
Operation Level	Target on Specific technical problem solving	Project Managers, engineers, risk assessment consultants	Function/Output: Technical analysis and enhancement on business units' security

6.3. Method implementation

After the structure of the risk assessment method has been decided, we come to the implementation part. This method will follow the ISO 27005 instructions in all three level of organization of conducting risk assessment. The thesis will use the operational level as an example to illustrate the implementation of the risk assessment process.

The main process for risk assessment according to ISO 27005 are 1) risk identification, 2) risk analysis, 3) risk evaluation and 4) risk treatment. In risk identification, we need to identify assets, threats, existing controls, vulnerabilities and consequences. In risk analysis, we will decide the methodology to measure risks, qualitative or quantitative. Then we assess the consequence and likelihood of the incident, and decide the level of risks. In risk evaluation, fuzzy theory will be applied to combine different experts' opinions, comparison will be conducted between the estimated risks criteria, and related factors will be considered for the evaluation. Risk treatment is the final step including risk modification, retention, avoidance, and sharing [41]. In the following we will establish the context and then discuss each step in order.

6.3.1. Preparation / Establishing the context

In this stage, the organization should define the goal of the risk assessment. It should meet the requirements of confidentiality, integrity and availability of the object, and support the business strategy at a higher level. Then the organization need to:

- Define the scope of the risk assessment,
- Develop criteria for the information system's risk assessment,
- Select an appropriate framework and standard for risk assessment. For this part we will use COSO ERM, AHP, Fuzzy theory and mainly based on the ISO 27K standards,
- Maintain or build sufficient communication channels between the upper level of the management board with the lower level of technical teams. Thus the team can have full support and enough information to carry out the risk assessment.

Human factor is also an important issue. Establishing a competent team is vital to the success of the RA process. The team is usually led by the head of project, who has sufficient knowledge in the risk assessment area, and has excellent coordination skills. The team also involved people with related technical background for risk assessing. It might be good to have an official certificated person for certain RA standards or tools according to the risk assessment requirement. External consultants can be helpful when necessary. To decide if external consultants are needed or not, and how many of them are needed, an evaluation form can be used from [42] to judge which type of approach the risk assessment project belongs to, in-sourcing, partial outsourcing or full outsourcing,. In-sourcing RA approach will not involve any external consultant, full outsourcing RA approach will need enough external consultants to take over the whole project, while partial outsourcing RA approach will need some external consultants depend on the project requirement. Sometimes more than one expert is involved in the team and they will give out different opinions for the risk assessment. In this case fuzzy theory can be applied to achieve a balanced result, which will be discussed in the section 6.3.3.

6.3.2. Risk identification

Risk identification is to identify the information system's assets, threats and vulnerabilities. The concepts of these elements have been introduced in section 4.1. Risk identification is mainly in charge of collecting data for the later risk analysis. In the ISO 27005 document Annex B [41] is given an example of identification and evaluation of assets and impact assessment. The reader can refer to the standard for a more detailed description. This chapter will not cover all types of assets in information systems but only the operational level, as given an example to show how the identification is done, the similar identifications process apply to the assets in organizational and business level as well. For the assets identification data collection, experts opinion is highly valued. In order to get more accurate results the Delphi method can be used, which is introduced in 4.3. In other cases some general survey methodologies might be applied, such as questionnaires, interviews of staff and users, physical inspection or document analysis [41]. The following part will present risk identification process.

a. Analyze system components: This step is to analyze information systems (on operational level here) and different subsystems, within the RA scope as defined previously, and according to the organization structure and business process. It would be clearer to have a system topology map. A network topology system is a good example. In order to cover all the risks for a complete information system, we not only should consider the network components, but also software, environment and so on. A clear system structure and on identified protection requirement level for the different parts will make the assets and control identification process more easy.

b. Identify assets: We will identify assets according to the definition introduced in 3.1.1. Based on an analysis of the system, an assets catalog can be collected. Then we will assign values to assets, based on the three attribute: confidentiality, integrity, availability. There are qualitative or quantitative ways to do this, in ISO 27005 Annex B2 there is an example shows how this could be done.

c. Identify threats: Threat identification will be done based on the definition introduced in 3.1.2. In ISO 27005 Annex B3 there are some typical threats to information systems that are listed with sources and consequences. It will be helpful to refer to this or other professional libraries/databases and compare with the identified assets. Some general survey methods stated in the beginning of chapter 6.3.2 can also be used. An assets-threats table can be drawn in this step. Then we assign the likelihood level to each threat, based on expert's experience (usually in levels) or some statistical data from previous activities.

d. Identify vulnerabilities: Vulnerability identification will be done based on the definition introduced at 3.1.3. Since vulnerability will not be affected if the threat does not happen, we can have this step after identification of threats. Beside the normal survey methods mentioned in the beginning of this chapter, some technical methods such as automated vulnerability scanning tools, security testing and evaluation, penetration testing, code review can be used [41]. An impact value will be assigned to the vulnerable part depending on how serious the consequence is. After this step, we can have a table of the relation between assets, threats and vulnerabilities.

e. Identify existing controls: According to ISO 27005, existing risk controls can be identified from documentation of controls and risk treatment implementation plans. There are two types of risk controls, 1) prevention for potential threats that not happen yet, and 2) protection for already existing vulnerabilities. It is not easy to assign a value to this part, but a list of existing controls and usages status will be achieve, and it will help better assess the likelihood and impact when a threat actually takes advantage of a vulnerability.

Fig 10 shows the structure of all the elements that are needed to be identified for risk assessment in the information system.

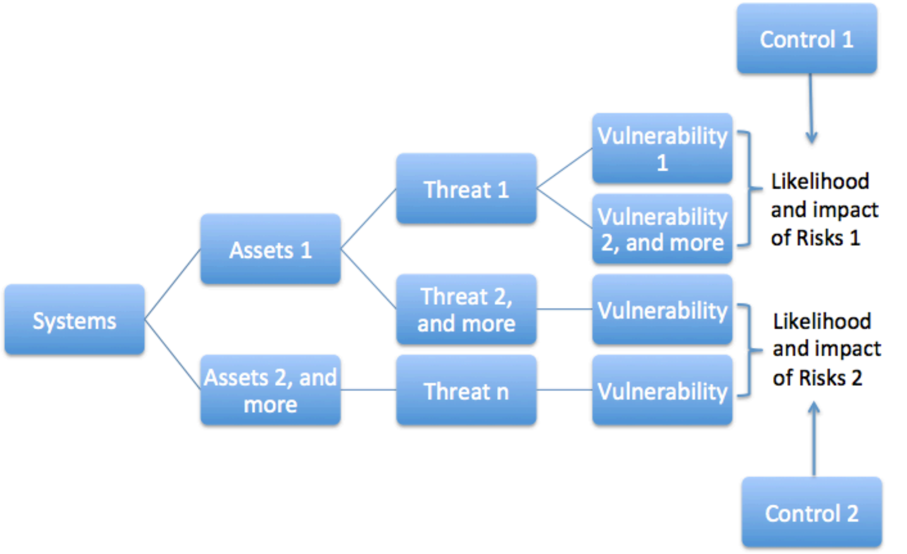


Figure 10. Relations of different criteria of risk assessment

After the identification, we should be ready for the next step, the analysis and evaluation part. According to ISO 27005 the data collection part for each element is done in the risk analysis, step. However we deal with here for thesis structure consideration. I will discuss this issue more in the next section as we combine risk analysis and evaluation together, something that I think is practical in real usage environment.

6.3.3. Risk analysis and evaluation

From previous step, we can have a clear map of the risk influence factors of the information system. Now we will evaluate each of the influence factors individually and comprehensively. This means for different valued influence factors we need to standardize the figures for comparison and consideration in order to come to a balanced conclusion. There are quantitative and qualitative methods to assess previous influence factors. In this section, we will use fuzzy theory. First we address a single value to each influence factors in the RA process and then give a comprehensive assessment of the whole risk. This is a typical approach when dealing with qualitative data that varies in a certain range. By overall analyzing the collected data, we can have a quantitative description of the final judgment. The detailed process will be showed in the following paragraphs. For risk assessment with many people's involvement, fuzzy theory is a mathematical way that can significantly unite various opinions with weights on basic requirement on the target, and get the best result in theory with little objective interference. There are other approaches to deal with quantitative values that this thesis will not cover. The reader should refer to papers that are related to the decision theory in RA process. In the structure each influence factor that belongs to same layer has different influence to the upper layer, so it is important to identify their weight as well. To identify the weight of each influence factor, the AHP method is applied. We have introduced it in section 4.3. It can show the relative importance of bottom factors to the total goal, by constructing an evaluation matrix and comparing factors with each other. Thus, it helps us to solve complex relations of influence factors and multi-level structured problems. AHP is a typical subjective weighting method that heavily depends on the decision maker's experience and judgment. Similar method is the Delphi method that combines experts' opinions in evaluation of the weight. There are also objective weighting methods such as the entropy method, which is usually more accurate and flexible, but also more time costly [43].

The AHP structure regarding the information systems show as the follows:

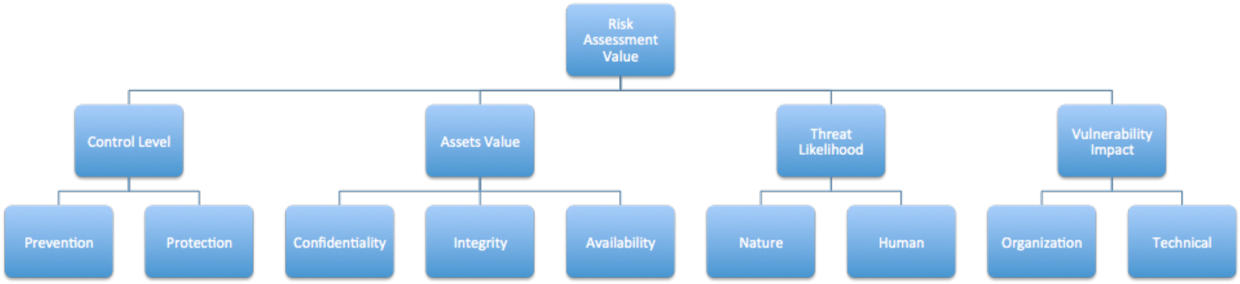


Figure 11. AHP structure of risk assessment

The first three AHP layers are defined: the top layer is the goal layer, the criterion layer, and the alternatives layer. Secondly, a pair-wise comparison will be conducted to calculate the weight of each influence factor to their upper level criteria [44]. For the criteria that have been identified, we take the criterion layer as an example, a judgment matrix can be derived from the expert's estimation. Following the proportion criteria theory, a nine-level comparison table will be derived:

Score (M)	Meaning
1	Two factors are equally important
3	One is moderate important than another
5	One is strongly important than another
7	One is very strong important than another
9	One is extremely strong important than another
2, 4, 6, 8	Median value supplement to previous judgment
1, 1/2, 1/3, … 1/9	Reciprocal value as the reverse importance compare with previous judgment

Then we can have a judgment matrix:

	Control	Assets	Threat	Vulnerability
Control	1	M_1	M_2	M_3
Assets	1/ M_1	1	M_4	M_5
Threat	1/ M_2	1/ M_4	1	M_6
Vulnerability	1/ M_3	1/ M_5	1/ M_6	1

In the judgement matrix, M_1 represents the importance level the Control factor, in analogy with the Assets factor in the RA process consideration. And $1/M_1$ represents the reverse relations, as showed in fig . The rest parameters are listed in the same way. Then we have the calculation matrix:

$$W = \begin{bmatrix} 1 & \mathrm{M1} & M2 & M3 \\ 1/M1 & 1 & M4 & M5 \\ 1/M2 & 1/M4 & 1 & M6 \\ 1/M3 & 1/M5 & 1/M6 & 1 \end{bmatrix}$$

To normalize the matrix we can get the weight set for these four factors (W_1, W_2, W_3, W_4). With each factor's weight being decided, an evaluation matrix will be made to combine different experts' judgments together. An evaluation matrix is showed as below:

$$R_g = \begin{bmatrix} R11 & R21 & R31 & R41 \\ R12 & R22 & R32 & R42 \\ \dots & \dots & \dots & \dots \\ R1j & R2j & R3j & R4j \end{bmatrix}$$

In the matrix, here R_{ij} is the evaluation of each risk factor that been assessed by each expert, where i represents four risk factors in our case: Control, Assets, Threats, Vulnerability, that influences the final information system's risks. And j represents the expert's series number. To quantify the risk factors expert could assign scales, 1 – 5 to each R_{ij}, where 1 indicates the least important and 5 indicates extremely important to the upper level criteria. If more detailed evaluation is needed we can have a 1 – 9 scaled systems as well. The final risk presents as:

$$R_{final} = W_g * R_g = (W_1, W_2, W_3, W_4) * \begin{bmatrix} R11 & R21 & R31 & R41 \\ R12 & R22 & R32 & R42 \\ \dots & \dots & \dots & \dots \\ R1j & R2j & R3j & R4j \end{bmatrix},$$

where W_g represents the weight of the four risk factors, as achieved in the judgment matrix, and R_g represents the opinion matrix assessed by the experts. For the sub-layers, the same method applies so the impact and likelihood of each influence factor to the goal would be very clearly identified, as showed in Table 11,

Table 11. Decision table for AHP analysis

First Layer Criteria	Evaluation	Second Layer Criteria	Evaluation
Control	R1	Prevention	S1
		Protection	S2
Assets	R2	Confidentiality	S3
		Integrity	S4
		Availability	S5
Threats	R3	Nature	S6
		Human	S7
Vulnerability	R4	Operational	S8
		Technical	S9

So the result is the comprehensive judgment from various experts regarding each influence factor. The final risk can be assessed from bottom up, layer by layer, with this method.

With the risk factors values identify, we can compare them with the previous criteria and finally decide the overall risk. In ISO 27005 Annex E2, three methods are recommend to do this. There are 1) a matrix with predefined values, 2) ranking of threats by measures of risk, and 3) assessing a value for the likelihood and the possible consequences of risks [41]. Since we already have the absolute values of the risk factors, but these values lack of practical meanings without analyzing in specific environment. Here the risk matrix would be a propel way to deal these factors.

		1			2			3			4			5			Likelihood of threats
		1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	Ease of Exploration
1	1																
	2																
	3																
2	1																
	2																
	3																
3	1																
	2																
	3																
4	1																
	2																
	3																
5	1																
	2																
	3																
Assets Value	Existing Control Level																

Figure 12. Overall risk matrix

In Figure 12, an achieved final risk assessment result will be mapped into the risk matrix, with its four risk factors in our case. With the help of risk matrix, the user can easily decide the risk level by checking where the result is located in the matrix.

In this section, a AHP-Fuzzy method is simply presented to analyze the overall risks value. There are many other methods to quantify risks. The reader can judge by the situation. For this AHP example structure, the practical cases might be more complicated or analyzed in a different way, the reader can use the method flexibly. The risk matrix might also exist in other forms, some people developed it in 3 axes, or with different attributes, but the same principle applies.

6.3.4. Risk Treatment and acceptance

After the risk analysis and evaluation, the next step is to deal with the achieved risks results. Since this thesis is focused on risk assessment methodology and process, this section will only briefly introduce the risk treatment in practice. There are four parts of risk treatment, Mitigation, Transfer, Avoidance, and Retention of risks [45], as described in section 3.3. For achieved risks information, the user can prioritize risks according to the risk matrix, make plans and take extra control measures to deal with the risks, based on cost effect analysis. Documentation is usually necessary in this step. But one tricky problem that lies in front of risk treatment is how and to what level to accept risks. According to the risk matrix presented in ISO27005, if the risk assessment is conducted in a qualitative way, then three types of risks might be categorized: unacceptable risks, acceptable risks, and neutral area. For the first two categories the decision making is obvious. To decide the acceptance of risks located in the neutral area, a so called ALARP analysis can be applied. It stands for “As Low As Reasonably Practicable”, and it also based on cost benefit principle. A simple illustration will be shown as in Figure 13.

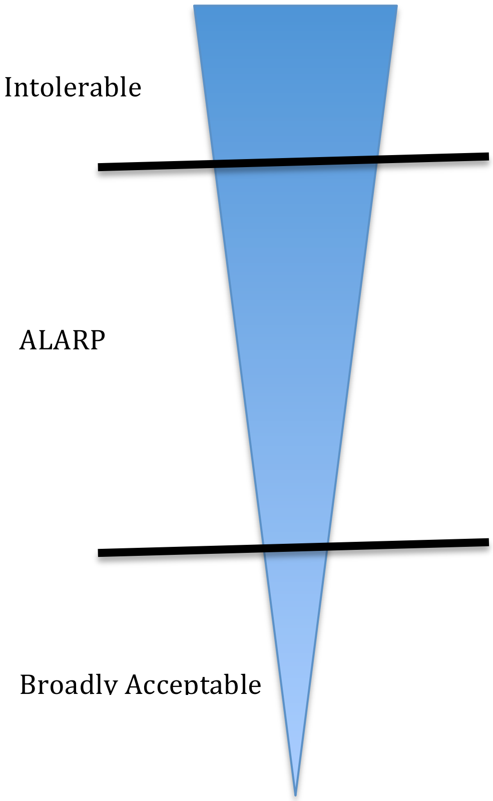


Figure 13. The ALARP model

In the intolerable area, risks are too high so the user has to concentrate to deal with these risks. In the broadly acceptable area, risks are negligible because it is not worth to take care of them. In the ALARP area, for qualitative analysis, a further cost benefit analysis will have to be made, in order to decide if further investment is needed [46].

In the end a risk assessment report will be formed based on the previous work. It will be conducted in time, so the risk can be under control. It will follow the three levels structure, Organization level, Business level and Operational level. The report covers all the methods being used, the results being achieved, the scope and area being assessed, the responsible people, and references. The report should also give out analysis for each finding, not only the results and conclusions, but some suggestions can also be given out depending on the requirements of the RA process.

6.4. Remaining Problems

The proposed methodology in the thesis basically follows ISO 27K guidance. Even though this standard is internationally recognized and widely used now, there are still some inevitable problems that remain. This is for various reasons, such as insufficient environment to carry out all the processes, limitedness of organizational structure and resources. Obscure description of the process in the method/standard can also cause trouble, though this might be depending on the situation. For example, on what level should the organization identify assets? Too large would lead to less accuracy, too small would be time consuming. Identification of threats and vulnerabilities would also give similar problems. The same threats can affect different assets, but depending on existing vulnerabilities and which controls that are in place, the impact might vary. So it is very important to consider these issues in general. It is difficult to put this into rules. Thus, it might affect the result or cause extra trouble for an inexperienced evaluator. Experience would definitely be of value in such a situation.

Another problem is that, as the thesis presents an RA structure that covers three levels of organizational activities in information risk assessment, a vertical solution is formed. But according to the information systems development life cycle, there are five phases: initiation, acquisition/development, implementation/assessment, operations/maintenance and disposal [51]. Therefore, a horizontal and timely view of the RA process is not showed in this solution. In each phase of the life cycle, there are different RA requirements and goals, and the RA procedure and activities should be identified according to each phase. However the detailed solution regarding to each phase will have to be studied in future work.

7. Conclusion

The purpose of the thesis was to survey risk assessment (RA) methods, and help the user solve RA problems using best practice. The thesis has presented characteristics of various commonly used RA methods, and compared them in different dimensions. A decision framework was proposed to help the user decide the best method for the RA process. If the user is not sure about whether any existing method is suitable for his environment, a specific method can be developed. Consequently, I have presented an example of a self-developed RA process. As mentioned before, the self-developed method is a more systematic method and covers the whole level of risk assessment instead of focusing on a single point of the problem. It is based on practical design so that it can be used in the industry. The idea was to present a detailed process of risk assessment, based on a combination of existing RA methods. In the industral environment the commonly used risk assessment methods have more or less followed the ISO standard or other standards and been tested by the market. Readers can choose their own method according to the decision framework introduced in section 5.3, or develop their own method which follows a certain standard, according to the process introduced in chapter 6. Information systems are more complicated nowadays and require more sophisticated methods to ensure the organizational and business security. There will always emerge more challenges in the system development lifecycle, so keeping a good security environment and culture by conducting risk assessment is important. This will need the operator’s knowledge, experience, rigor and flexible judgement, seamless cooperation, and great patience. The thesis will assist in the RA process for information systems and guide the user to a more efficient work.

Appendix A.

Risk assessment methodology analysis for the decision framework

In this appendix, Risk assessment tools and methodologies are analyzed according to the criteria introduced in the decision framework in section 5.2. One RA tool or method is analyzed in each table. Each table is divided into two parts. The first part evaluates the cost/effect criteria, which includes quantitative or qualitative, time, human factors and usability. The second part evaluates the environmental criteria, which includes scope, flexibility, standards' compliance and purchase price. For each criterion of the RA tool or method we will give out the analysis of the tool or method regarding that criterion, then a value will be assigned to the criterion (only to cost/effect criteria). With all the criteria of every methods being analyzed, the user can quickly look up in the appendix A and receive a quantified result to decide about the best approach for the risk assessment project within their requirements.

FTA	Assigned values and explanations
Quantitative or qualitative	Both. 2
Time	Getting exact numbers for the probabilities leading to the event is usually impossible for the reason that it may be very costly and time consuming to do so. But software can ease the situation now [52]. 2
Human factor	An engineer with a wide knowledge of the design of the system or a system analyst with an engineering background is the best person who can help define and number the undesired events. But would involved different position people, such as system designer, system analysts, testers, etc 2
Usability	The method uses Boolean logic, probability calculation, complicate logic relations, probability rate for each event could be hard to get. 1
Scope	Covers the whole RA process, including the design phase, facility modifications and operation. Broad scope
Flexibility	FTA is very good at showing how resistant a system is to single or multiple initiating faults. And both internal and external events. Very good flexibility, can be quantitative when every bottom event know the probability, otherwise can be qualitative, depends on the complexity
Standards Compliance	BS7799/ISO27k
Purchase price	Free

ETA	
Quantitative or qualitative	Both. 2
Time	Could be time consuming, Addresses only one initiating event at a time. 2
Human factor	Requires at least one expert with practical training and experience. 3
Usability	Involves probability calculation with selected path. 2
Scope	Covers the RA process from design phase, facility modifications and operation. Broad scope
Flexibility	Enables the assessment of multiple, co-existing faults and failures, organization. flexible
Standards Compliance	IEC 61025 [47]
Purchase price	Free

Delphi	
Quantitative or qualitative	Qualitative 1
Time	Involves several rounds of processing, group discussing, time consuming 1
Human factor	Many staff involved, some experts required but not necessary from outside 2
Usability	Quite clear and easy process 3
Scope	Can be used in many situations Broad
Flexibility	For complicated environment No flexibility
Standards Compliance	N/A
Purchase price	Free

AHP	
Quantitative or qualitative	Both 2
Time	3-step process, with modeling and calculation 2
Human factor	No special requirement 1
Usability	Not complicated Metric calculation 2
Scope	Can be used in many environment Broad
Flexibility	AHP usually can combine with Fuzzy logic, and could be quite flexible in the areas of using, can cover the whole systems risk assessment. Flexible
Standards Compliance	bs7799 / ISO27k
Purchase price	Free

FMECA	
Quantitative or qualitative	Both 2
Time	Involved with large data set, even though usually serves as input to other systematic method, so it doesn't need to cover different stage of the system risk assessment 2
Human factor	Should involve with system designer with different part, with the assistant of quality controller, will need group work and cooperation 2
Usability	Mathematical calculation of Criticality Analysis: Cm= $\beta * \alpha * \lambda p*t$ *-MTain Failure Modes Effects ans Criticality Analysis Notes* *2*
Scope	Covers from the design phase, facility modifications and operation Implemented early in the design phase, and will effectively influence the final system configuration Broad
Flexibility	FMECA is good at exhaustively cataloging initiating faults, and identifying their local effects. It is not good at examining multiple failures or their effects at a system level. [53] Not so flexible
Standards Compliance	This alternative does not consider combined failures or typically include software and human interaction considerations. It also usually provides an optimistic estimate of reliability. Therefore, FMECA should be used in conjunction with other analytical tools when developing reliability estimates. [54]
Purchase price	Free

OCTAVE	
Quantitative or qualitative	Qualitative 1
Time	Values for impact and probability 1
Human factor	OCTAVE is a flexible and self-directed risk assessment methodology. A small team of people from the operational (or business) units and the IT department work together to address the security needs of the organization. The team draws on the knowledge of many employees to define the current state of security, identify risks to critical assets, and set a security strategy. It can be tailored for most organizations. 3
Usability	3
Scope	Mainly for information systems Narrow
Flexibility	Each method can be tailored to the organization's unique risk environment, security and resiliency objectives, and skill level. Flexible
Standards Compliance	N/A
Purchase price	Free

CORAS	
Quantitative or qualitative	Qualitative 1
Time	Includes 7 steps, but each one is not very complicated 2
Human factor	Do not have specific requirement for people 3
Usability	No complicated calculation, model based using UML 3
Scope	Majorly for information systems security Narrow
Flexibility	Integrated approach to system design and risk analysis Flexible
Standards Compliance	ISO 31k, ISO 27k, AS/NZS 4360
Purchase price	Free

CORA	
Quantitative or qualitative	Qualitative 1
Time	Two steps process 3
Human factor	CORA uses external risk experts to perform the risk analysis, 1
Usability	User-friendly program interfaces include instructions and data entry guidance. Very stable usage environment since the method was started to be used in 1978. 3
Scope	Applies to all kinds of risk Broad
Flexibility	Single loss value, then add up Not flexible
Standards Compliance	N/A
Purchase price	$7,000 to $85,000

COBRA	Currently under re-development, Unable to purchase right now
Quantitative or qualitative	Both 2
Time	Not very time costly since it is a questionnaire based system with mature software support 3
Human factor	Can be taken by organization itself, no outside requirement 3
Usability	Based on PC tools and expert system principles, but new version not available now 1
Scope	Broad
Flexibility	Flexible
Standards Compliance	ISO 17799 → ISO 27k
Purchase price	$895 (for ISO 17799 only) / $1995 (Full suit)

Risk Watch	
Quantitative or qualitative	Both 2
Time	Predefined models and expert database 3
Human factor	No external specialist needed 3
Usability	Easy to use with mature business solutions 3
Scope	Can cover 5 area, not only information systems Broad
Flexibility	Can analysis organization, facilities, systems, applications, networks, etc Flexible
Standards Compliance	ISO 27k, ISO 32k, and other stands
Purchase price	$15000

FRAP	
Quantitative or qualitative	Qualitative 1
Time	Simple and fast 3
Human factor	Includes owner, project lead, facilitator, scribe, team members No external people needed, but people should understand the process and brainstorm 2
Usability	Easy to use, least costly 3
Scope	Mainly for computer and software company Narrow
Flexibility	Mainly on the systems that requires time and cost reduction one system at a time Not flexible
Standards Compliance	ISO 17799 → ISO 27k
Purchase price	Free

COSO ERM	
Quantitative or qualitative	*Risk assessment techniques*. Risk assessment methodologies comprise a combination of qualitative and quantitative techniques. An example of the use of qualitative risk assessment is the use of interviews or group assessment of the likelihood or impact of future events. Quantitative techniques include probablistic and nonprobabilistic models. Probabilistic models are based on certain assumptions about the liklihood of future events. Nonprobabilistic models such as scenario-planning, sensitivity measures, and stress tests, attempt to estimate the impact of events without quantifying an associated likelihood [48]. Both
Time	Need to consider all the aspect and all the level in an enterprise, see the model 1
Human factor	Need specialist 2
Usability	Practical, sustainable and understandable 3
Scope	Covers all levels and all stages in an organization’s activities Broad
Flexibility	For organizations and thorough assessment Not flexible
Standards Compliance	2010.A1, 2120.A1, 2210.A1
Purchase price	Cost

@Risk	
Quantitative or qualitative	Quantitative 2
Time	Based on Monte Carlo Simulation, with Microsoft excel support 2
Human factor	No special requirement 3
Usability	Mature product 3
Scope	Not only IT security Broad
Flexibility	Enables to simulate models with a variety of scenarios Flexible
Standards Compliance	N/A

References

[1] IEC/ISO 31010, “Risk management – Risk assessment techniques,” INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2009

[2] A. Rot, “IT Risk Assessment: Quantitative and Qualitative Approach,” proceedings of the World Congress on Engineering and Computer Science, 2008

[3] G. Stonebumer, A. Goguen, and A.Feringa, “Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology,” National Institute of Standards and technology, Special Publication 800-30, 2002

[4] S. Kaplan, and B. J. Garrick, “On The Quantitative Definition Of Risk,” Risk Analysis, Vol. 1, No. 1, 1981

[5] T. J. Altenbach, “A comparison of Risk Assessment Techniques from Qualitative to Quantitative,” ASME Pressure and Piping Conference, 1995

[6] B. Karabacak, and I. Sogukpinar, “ISRAM: information security risk analysis method,” Computer & Security 24, pp. 147-159, 2005

[7] L. Willcocks, and H. Margetts, “Risk assessment and information systems,”

[8] J. Bisson, and R. S. Germain, “The BS 7799 / ISO 17799 Standard For a better approach to information security,” White Paper

[9] C. Schou, “Information Assurance for the Enterprise: A Roadmap to Information Security,” McGraw-Hill/Irwin, 1st edition, 2006, Chapter 15

[10] http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment, European Union Agency for Network and Information Security, Retrieved 2014

[11] Loudon K, Loudon J. Management Information Systems: A Contemporary Perspective. Macmillan, New York, 1991.

[12] H. A. Linstone, M. Turoff, and Olaf Helmer, “The Delphi Method Techniques and Applications,” ISBN 0-201-04294-0, 2002

[13] J. Rees, and J. Jaisingh, “Value at Risk: A methodology for information Security Risk Assessment,” CERIAS Tech Report 2001-127

[14] M. P. Kailay, and Peter Jarratt, “RAMeX: a prototype expert system for computer security risk analysis and management,” Computers & Security 14, 1995

[15] ISO/IEC 27002:2013, “Information technology – Security techniques –Code of practice for information security controls,” ISO & IEC, 2013 (Previous ISO17799:2005)

[16] ISO/IEC 27001:2013, “Information technology –Security techniques – Information security management systems – Requirements,” ISO & IEC, 2013 (Previous ISO/IEC27001:2005, BS7799)

[17] FIPS PUB 199, “Standards for Security Categorization of Federal Informaion and Information systems,” NIST Information Technology Laboratory, 2004

[18] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, “Introduction to the OCTAVE Approach,” Carnegie Mellon Software Engineering Institute, 2003

[19] Palisade Corporation, “@RISK: A Hands-On Tutorial,” 2011

[20] T. Dimitrakos, B. Ritchie, D. Raptis, and K. Stolen, “Model based Security Risk Analysis for Web Applications: The CORAS approach,” Euroweb 2002

[21] BS IEC 61882:2001, “Hazard and operability studies (HAZOP studies) – Application Guide,” IEC, 2001

[22] F. D. Braber, G. Brendeland, H. E. I. Dahl, I. Engan, I. Hogganvik, M. S. Lund, B. Solhaug, K. Stolen, and F. Vraalsen, “The CORAS Model-based Method for Security Risk Analysis,” SINTEF, 2006

[23] K. Lin, and K. E. Holbert, “PRA for Vulnerability Assessment of Power System Infrastructure Security,” Power Symposium, 2005

[24] E. J. Henley and H. Kumamoto, “Probabilistic Risk Assessment,” IEEE Press, pp.8-43,New York, 1991

[25] H. Kumamoto and E. J. Henley, “Probabilistic Risk Assessment for Engineers and Scientists,” IEEE Press, pp.95-115,New York, 1996

[26] CCPs 1992, “Guidelines for hazard evaluation procedures, second edition,” Centre for chemical process safety, American institute of chemical engineers, 1992 (book P276)

[27] World Health Organization, “Risk characterization of microbiological hazards in food, Guidelines”, FAO/WHO, 2009

[28] C. Bazzani and M. Canavari, “Forecasting a scenario of the fresh tomato market in Italy and in Germany using the Delphi method,” British Food Journal, 2013

[29] A. Vorster and L. Labuschagne, “A Framework for Comparing Different Information Security Risk Analsysis Methodologies”, SAICSIT, 2005

[30] David Gossman, “Hazop – Pros and Cons”, http://gcisolutions.com/gcitn0309.html, Retrieved 2014

[31] A. Behnia, R. A. Rashid and J. A. Chaudhry, “A Survey of Information Security Risk Analysis Methods”, Smart Computing Review, 2012

[32] “FAQ: ISMS risk management”, http://www.iso27001security.com/html/risk_mgmt.html, Retrieved 2014

[33] “COBRA Module Manager”, http://www.security-risk-analysis.com/modman.htm, Retrieved 2014

[34] T. R. Peltier, “FACILITATED RISK ANALYSIS PROCESS (FRAP)”, Auerbach Publications, 2000

[35] “Enterprise Risk Management — Integrated Framework: Executive Summary”, Committee of Sponsoring Organizations of the Treadway Commission, 2004.

[36] COSO ERM, http://www.grc-resource.com/?page_id=32, Retrieved 2014

[37] Riskwatch, http://riskwatch.com, Retrieved 2014

[38] U.S.NRC, “Tutorial on Probabilistic Risk Assessment (PRA)”, Retrieved 2014

[39] ISO/IEC 27000:2014, “Information technology-security techniques – information security management systems-overview and vocabulary”, ISO & IEC, 2014

[40] “iso 31000 and iso 27001 how are they related”, http://www.iso27001standard.com/blog/2014/03/31/iso-31000-and-iso-27001-how-are-they-related/, Retrieved 2014

[41] ISO/IEC 27005:2011, “Information technology-security techniques-information security risk management”, ISO & IEC, 2011

[42] IAAITC, ENISA, MEA-I, “Risk management & IT security for Micro and small business”, 2007

[43] T. Chen and J. Freeman, “Using AHP-Entropy weight and TOPSIS methodology in green supplier selection”, EurOMA 2014 Conference, 2014

[44] M. C. Lee, “Information Security Risk Analysis Methods and Research Trends/ AHP and Fuzzy Comprehensive Method”, IJCSIT, 2014

[45] ENISA, “Risk assessment and risk management methods: Information Packages for small and Medium sized Enterprises (SMEs)”, 2006

[46] ALARP, http://www.hse.gov.uk/risk/theory/alarpglance.htm, Retrieved 2015

[47] “Risk Analysis, Risk Assessment, Risk management”, http://www.nr.no/~abie/RiskAnalysis.htm, Retrieved 2014

[48] Enterprise Risk Management—The COSO Framework: A Primer and Tool for the Audit Committee, 2010 AICPA

[49] Silvianita, M. F. Khamidi and K. V. John, “Critical Review of a Risk Assessment Method and its Applications”, IACSIT, 2011

[50] M. C. Lee, “Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method”, IJCSIT, 2014

[51] S. Radack, “The system development life cycle”, NIST

[52] FTA, http://en.wikipedia.org/wiki/Fault_tree_analysis, Retrieved 2014

[53] FMECA, http://en.wikipedia.org/wiki/Failure_mode,_effects,_and_criticality_analysis, Retrieved 2014

[54] “Research and Development Accomplishments FY 2004”, Federal Aviation Administration, 2004, Retrieved 2014