A Review of Research on Risk Analysis Methods for IT Systems

Sardar Muhammad Sulaman  
Department of Comp. Science  
Lund University  
Sweden  
sardar@cs.lth.se

Kim Weyns  
Department of Comp. Science  
Lund University  
Sweden  
kim.weyns@cs.lth.se

Martin Höst  
Department of Comp. Science  
Lund University  
Sweden  
martin.host@cs.lth.se

ABSTRACT

Context: At the same time as our dependence on IT systems increases, the number of reports of problems caused by failures of critical IT systems has also increased. This means that there is a need for risk analysis in the development of this kind of systems. Risk analysis of technical systems has a long history in mechanical and electrical engineering.

Objective: Even if a number of methods for risk analysis of technical systems exist, the failure behavior of information systems is typically very different from mechanical systems. Therefore, risk analysis of IT systems requires different risk analysis techniques, or at least adaptations of traditional approaches. This means that there is a need to understand what types of methods are available for IT systems and what research that has been conducted on these methods.

Method: In this paper we present a systematic mapping study on risk analysis for IT systems. 1086 unique papers were identified in a database search and 57 papers were identified as relevant for this study. These papers were classified based on 5 different criteria.

Results: This classification, for example, shows that most of the discussed risk analysis methods are qualitative and not quantitative and that most of the risk analysis methods that are presented in these papers are developed for IT systems in general and not for specific types of systems, like e-government systems.

Conclusions: The results show that many new risk analysis methods have been proposed in the last decade but even more that there is a need for more empirical evaluations of the different risk analysis methods. Most papers were identified that propose new risk analysis methods, but few papers discuss a systematic evaluation of these methods or a comparison of different methods based on empirical data.

Categories and Subject Descriptors

H.1.0 [Information Systems]: Risk analysis and management

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

EASE ’13, April 14 - 16 2013, Porto de Galinhas, Brazil  
Copyright 2013 ACM 978-1-4503-1848-8/13/04 ...$15.00.

Keywords
Risk Analysis, IT systems, Mapping study

1. INTRODUCTION

IT systems have become an essential part of our modern society. This evolution has not only created new opportunities, but also new threats to our society. The presence of IT systems everywhere has made us dependent on IT systems for our daily life. This is the case both for individuals and organizations, both private as well as public organizations. However, at the same time as the usage of, and dependence on IT systems increases, the number of reports of problems caused by failures of critical IT systems has also increased [8].

One of the common aspects of these failures is the faith in systems that are not sufficiently dependable. The core of this problem is not that these systems suddenly become unreliable, but that we have become critically dependent on a variety of systems without analyzing whether they are dependable enough and what the consequences could be of a possible failure [18]. To prevent critical systems from causing problems for the organizations dependent on them, risk analysis is a necessary activity.

Risk analysis of technical systems has a long history in mechanical and electrical engineering where many well-established methods exist. The failure behavior of IT systems is typically different from mechanical systems and, at the same time, the complexity can be significantly higher. The high rate at which new IT systems are being developed and updated for many critical applications usually means there is not enough historical data available for a strictly statistical analysis of the reliability of each system and its components, as is sometimes the case in risk analysis of mechanical systems.

For all these reasons, risk analysis of IT systems requires different risk analysis techniques or at least adaptations of these traditional risk analysis approaches. In this article we present a systematic overview of previously published research on risk analysis for IT systems.

Risk analysis can be performed during the development of the system, at deployment of the system or at any time afterwards. In the ideal situation, the risk analysis should be re-evaluated each time major changes occur in the system or in the environment in which the system is used.

In this article we present an overview of operational risk analysis methods for IT systems. This includes many different types of systems and methods, but does not include project risk analysis methods, used to analyses the project
management risks in software development projects.

Section 2 presents related work in the field of risk analysis and systematic literature reviews. Section 3 discusses the methodology used in this study in detail. Section 4 contains the special measures that were taken to improve the validity of this research. Next, Section 5 contains the results of this mapping study and presents the categorization of the identified articles based on different attributes of the research and the risk analysis methods presented in each article. Finally, Section 6 summarizes and analyses the results of this classification.

2. RELATED WORK

Many different national and international high-level frameworks exist for information technology risk management and assessment. Such frameworks have for example been published by the International Organization for Standardization (ISO), such as ISO/IEC 27005 [7] and ISO/IEC 27002 [6], by national governmental organizations, such as the National Institute of Standards and Technology (NIST) [21] or the British Central Communication and Telecommunication Agency (CCTA) [5], by non-governmental organizations such as Club de la Sécurité de l’Information Français (CLUSIF) [16] or by research institutes such as the Carnegie Mellon Software Engineering Institute (SEI) [1]. A detailed comparison of some of these frameworks can for example be found in [3] and [22].

There also exist a number of low-level risk analysis methods for technical systems in general or for IT-systems in particular. Some of the most well-known methods are Fault Tree Analysis (FTA) [4], Failure Mode and Effect Analysis (FMEA) [15] and Hazard and operability study (HAZOP) [19]. Some of the frameworks mentioned above specifically recommend one or more of these risk analysis methods.

The goal of the study presented in this article is to identify research articles that describe or evaluate new or established risk analysis methods for IT systems, which includes both high- and low-level methods. To identify and summarize these research articles this study uses a methodology of mapping studies [11], which includes a definition of systematic literature reviews [12].

Systematic literature reviews and mapping studies have been conducted in different studies [10] in widely different areas such as cost estimation (e.g. [8]), open source software (e.g. [20]), and testing (e.g. [11]). The systematic reviews, [14] and [9], have focused on project risk assessment in software development projects. However, to the best of our knowledge, no reviews have looked specifically at operational risk analysis methods for IT systems.

3. METHODOLOGY

This article presents a study of available risk analysis, assessment, and management methods for IT systems. The review presented here is a systematic mapping study, conducted based on the guidelines presented in [12]. This article presents, in addition to the overview of the identified risk analysis methods, a categorization of the identified methods.

A review protocol was developed in the initial phase of the review. It contains research background, research questions, search strategy, study selection criteria and procedures, validity assessment, data extraction instructions, and data synthesis strategies.

Figure 1: Identification and selection of articles.

This research is conducted as a planned study and was carried out in the following steps:

1. Defining the research questions.
2. Selection of sources to be searched for relevant articles.
3. Defining the search query and performing the search on the selected sources, resulting in 1203 articles.
5. Defining the inclusion and exclusion criteria and initial selection based on titles and keywords according to the defined criteria, leaving 320 articles for the next steps of the study.
6. Second round of selection by reading abstracts according to the same criteria and first classification of the articles, leaving 200 articles for the next steps of the study.
7. Final selection of articles based on careful reading of the full text of each article, resulting in a final list of 57 relevant articles for this study.
8. Analysis of the results of the classification of the final list of articles.

During each step special measures were taken to improve the validity of the research. Each step is described in more detail in the following subsections.

The steps involved in the identification and selection of articles are summarized in Figure 1.

3.1 Research questions

The objective of this article is, as described above, to present an overview of risk analysis methods for IT systems, by summarizing and synthesizing the results from research that has already been carried out on available risk analysis.
methods for IT systems. This general goal has been broken down to the following main research questions:

1. What risk analysis methods and approaches are reported in the research literature for IT-systems?
2. To what extent are the identified methods used in practice?
3. Is there empirical research published where the identified methods are evaluated/compared/etc.? If there is, which research methodologies are used?
4. Which phases of the risk management process have been the focus of the identified research articles?
5. What type of risk analysis methods are presented in the published research, qualitative or quantitative?

This research can be categorized as a systematic mapping study that is carried out in the same way as a systematic review. It focuses on the main research that has been conducted in the area of risk analysis for IT systems, and it is done by adopting a systematic approach to identify relevant research and classify the identified research articles according to predefined categories.

3.2 Search strategy

Searched resources

The following databases were searched (through Engineering Village\(^1\)) for relevant research:

- **INSPEC**: This database is provided by Elsevier Engineering Information Inc. and the Institute of Electrical Engineers (IEEE). It includes articles from 1969 to present.
- **COMPENDEX**: This database is provided by Elsevier Engineering Information Inc. It includes papers from 1969 to present.

The above mentioned databases provide a broad coverage of the area of interest, i.e. “Risk analysis methods for IT systems”, and they include articles from the main conferences, journals, and publishers (IEEE, ACM, Springer, etc.).

Search query

After a number of iterations, the following search query was considered a good compromise between finding as many of the relevant articles as possible, and returning a manageable number of results:

\[
\{(\text{risk analysis}) \text{ OR } \text{risk analyses}) \text{ OR } \text{risk identification}) \text{ OR } (\text{RA})\}
\]

\[
\text{AND } (\text{method}*) \text{ OR } \text{technique}*) \text{ OR } \text{approach}*)
\]

\[
\text{AND } (\text{computer system}) \text{ OR } \text{information system}) \text{ OR }
\]

\[\text{http://www.engineeringvillage2.org}\]

The search string has four main parts separated by AND and NOT clauses.

The first part of the search string excludes articles that are not about ‘risk analysis’ or ‘risk identification’.

The second part of the search string excludes articles that do not discuss one or more specific methods for risk analysis, or a synonym to ‘method’. The ‘*’-character is a wildcard representing any string of characters, which allows different grammatical numbers of the term to be identified, e.g. both ‘method’ and ‘methods’.

The third part of the search string excludes articles that are not in the field of information technology or computer science. The ‘*’-character is a wildcard representing one character, included because we want to identify both ‘-’ and ‘-’.

The last part of the search string explicitly excludes articles about oil, gas, agriculture or chemistry. These research fields traditionally have a strong safety focus and contain many papers about risk analysis. They are, however, not domains in which IT systems are considered as the most critical components, and this part of the search string was excluded to prevent irrelevant papers from these domains from dominating the returned results.

3.3 Inclusion and exclusion criteria

When articles were identified with the search string from the databases, it was necessary to manually remove non-relevant articles from the selection. This was done first based on the title and keywords, then based on the abstract, and finally based on the full text. The inclusion and exclusion criteria were defined during the design of the review protocol. The manual selection of articles was carried out based on the following criteria:

- Articles not about methods for risk analysis or risk management of computer system were excluded from the selection.
- Articles about the risk analysis of system development projects were excluded from the selection. That is, articles about risk management of project risks were excluded. The focus in this article is on risks for the organization depending on the operation of IT systems, i.e. operational risk, not about the project risks associated with developing the systems.
- Articles specifically about the risk analysis of computer networks were excluded from the selection because the focus in this study is on risk analysis for complete IT systems not just the network component of the system. The excluded articles present risk analysis of network components such as, firewalls, intrusion detection systems, routers and implementation of security policies.
to cope with unauthorized access of data or resources, e.g., [17].

- Articles about the risk analysis of space systems, nuclear power plants, embedded medical devices, and military systems were also excluded from the selection. These domains have a long history of risk analysis methods, but these methods are often very time-consuming and mostly suited for embedded systems that are analyzed in great detail. This study, however, focuses on risk analysis for large IT systems that are applicable to a wide range of systems in many types of organizations. An example of excluded article is [13].

Each of these criteria was necessary to limit the scope of this study. It would be impossible to cover risk analysis for all types of risk associated with all categories of IT systems in one review like this, because of the large number of relevant articles.

3.4 Selection of relevant articles

The above-mentioned search query was carried out on 23 May 2012 and retrieved 1203 articles, and it has been decided to continue systematic review with these records. After this, the title, keywords, abstract and author names were downloaded for the initial selection of relevant articles. Then the EndNote (Reference manager) was used for the removal of duplicate articles. It found (automatically) 91 duplicate articles that have been removed from the initial list. After this, 26 duplicate articles were found by manual search and removed from the initial list as well.

In each step of the selection process (based first on the title and keywords, then on the abstract and then on the full text) these criteria were used by the first author of this article to manually remove non-relevant articles from the initial selection. This resulted, in each step, in three groups of articles:

- **Relevant**: Articles that clearly fulfilled the criteria established above.
- **Not relevant**: Articles that were out of the scope of this study.
- **Possibly relevant**: Articles for which there was not enough information to establish whether they are relevant for this study. This list was checked by the co-authors for the selection. The remaining Articles (from selection based on title and keywords, and abstracts) were then added to the relevant articles for further selection in the next step.

After removing irrelevant articles based on the title and keywords, a first effort to remove non-relevant articles was carried out by the first author of this article. This selection resulted in a list containing 229 relevant and 48 possibly relevant articles. To check the reliability of this first step, the second author of this article cross checked 100 randomly chosen articles from the initial list and found disagreement on 3 relevant articles not added and 6 non-relevant articles added. To increase the reliability of the selection, it was therefore decided to repeat the initial selection process based on this information and to only exclude those articles that were not relevant in light of this. The selection process was by this conducted once again and resulted in 70 more articles from the initial list to the main selected list. After this, the possibly relevant articles list was checked and 21 out of 48 articles were selected and added in the main list for the next step of review. After doing the initial selection process again the resulted selection list came up with a total of 320 relevant articles.

The second selection was conducted based on the abstracts, the first author read the abstracts and found 183 relevant articles out of a total of 320. The second author again rechecked this selection and he found 17 more relevant articles. After adding these 17 articles the second selection list came up with a total of 200 relevant articles for the next step of review.

In the third step of the selection process, the full text of the relevant articles needed to be downloaded. The full text for all articles was not always available for all articles and 57 articles were removed from the selection because the articles were not written in English (most often in Chinese) or because the full text could not be downloaded (mostly older articles).

After this, the first author carefully read the full text of all downloaded articles and selected 77 relevant articles. The second author of this article cross-checked the excluded articles from the final list suggested adding two more relevant articles in the final list, which resulted in 79 relevant articles. Then, he cross checked the finally selected articles by reading the full text and removed 23 irrelevant articles. After removing the irrelevant articles the list contained 56 relevant articles. There was a disagreement for the selection [article 24], the third author carefully read it, and after discussion all authors agreed to select it for the review.

Finally, the reference lists of the most relevant articles were inspected for further relevant articles that were not included in the selection. Initially 5 articles were selected from reference inspection, after reading the full text of selected articles only one article identified as relevant for this study. This article was from a source that was not included in the searched resources. After adding this article the final list contains the 57 articles listed in the appendix of this article.

3.5 Data extraction and synthesis

In the final steps of the selection, i.e. the selection based on the full text of the articles, the articles were classified based in the following classes:

- **Class A** Articles describing or evaluating existing risk analysis methodologies.
- **Class B** Articles presenting improvements or changes to existing risk analysis methodologies.
- **Class C** Articles presenting new methods for risk analysis of IT systems.

Further, a number of relevant attributes were also extracted from each of the articles with respect to the research questions discussed in Section 3.1. The results of this data extraction and classification are discussed in Section 5.

4. VALIDITY ASSESSMENT

The main objective of this research is to summarize the available research in the field of risk analysis for IT systems. An important threat to the validity of this study is that it
cannot be guaranteed that all possible relevant articles in this field have been included in the study. First of all, only research published in English was included for practical reasons. Secondly, some lesser known journals or conferences are not available in the searched databases, and were therefore not searched in this study. Also, articles for which the full text was not available were excluded from this study. This mostly affects older articles. Thirdly, it is likely that some relevant articles were rejected by the search string, since it is impossible to define a search string that finds absolutely all relevant articles without returning an unmanageable number of false positives. Finally, it is of course also possible that relevant articles were incorrectly rejected during the manual selection process from over one thousand articles to the final selection of 57 articles.

To increase the validity of this study, the reference list of the most relevant articles from the final selected list were examined for missing important articles. This validity check resulted in only one new article being added to the selection of articles. This article had not been found in the automatic search because it was from a source not included in the searched databases.

In order to reduce the risk of incorrect rejection of an article during the selection process, the co-authors of this article cross-checked the selection in each step. Whenever there was doubt about whether to include an article or not, the article was retained for the next step of the selection process. After initial selection process based on the title and keywords, the second author of this article cross checked 100 randomly selected articles from the initial list, and suggested a few additions and removals of articles. Instead of just adding and removing these articles, it was decided to repeat the selection process and to keep any articles selected in either case.

After the second selection process based on abstracts, the second author of this article re-checked the complete selection and found 17 more relevant articles that had possibly been rejected incorrectly, and in this way made sure that also articles where we were in doubt were included.

After the third selection process that was conducted after reading the full text of articles, the second author of this article cross checked the finally selected articles by reading their full text and found 23 non-relevant articles according to the defined research questions.

That is, whenever there was a doubt in selection of an article it was retained for the next step, where more information was available to decide the relevance of an article with more accuracy. Whenever one author was not sure about the classification of an article, the co-authors reviewed the article and decision about the classification was based on the agreement by all authors.

By taking the above mentioned measures for the validity of this study we are more confident that most of the relevant articles for this study have been identified and included in the final list of articles.

5. RESULTS

This section presents an analysis of the data extracted from the selected articles. 5.1 Year of publication

In Figure 2, the publication year for the selected articles is displayed. It can be observed that the oldest selected article is from the year 1980, and the most recent from 2012. About half of the articles were published in the last 5 years before the publication of this study. That is, this indicates that the number of publications in the area has increased the later years, at least if we were able to find as many of the older articles as the newer articles.

5.2 Risk analysis method classification

Table 1 shows the classification of the selected articles into classes A, B, and C, see Section 3.5. Class A, about existing risk analysis methods, includes 18 articles. Articles in this class describe general risk analysis concepts and its importance for dependable IT systems. This class also contains some articles about the comparison of different risk analysis methods. Class B includes 5 articles that present improvements in existing risk analysis methods. The majority of the articles are in class C. It includes 34 articles that are about presenting new frameworks, methods and models for risk analysis.

5.3 Types of systems

Table 2 shows the types of system that the selected articles focus on. The majority of the selected articles, 49 articles out of 57, are about risk analysis of IT systems in general. This means that the paper does not specify which type of systems the research is about, and thereby it can be assumed that the intention is that the research results should be generally valid. However, 2 articles are specifically about risk analysis for e-commerce systems, 3 are about hospital sys-
5.4 Analytical or empirical research

In Table 3, the research methodologies that were used in the selected articles are categorized as either completely analytical (not containing any research based on the application of a risk analysis method on an actual system) or empirical (containing an explicit description of an application of at least one risk analysis method, either in a real-life setting or in a controlled experiment). 36 articles were identified as analytical and 21 as empirical research. These 21 articles all presented case studies on risk analysis methods, no surveys or experiments were identified.

5.5 Area of risk management

Risk management is a process that consists of several activities: risk identification, risk analysis, risk assessment, risk prioritization, and risk mitigation. It is a process that tries to find a balance between loss prevention and cost associated with countermeasures. It usually starts with the risk identification activity to determine a list of possible risks. Next, risk analysis is applied to combine the probability and the expected consequences associated with each risk. Sometimes the term ‘risk analysis’ is also used to include the risk identification step. Then, in risk prioritization all the identified risks are prioritized based on the results of the risk analysis. Finally, risk mitigation, dealing with implementing appropriate measures and controls to reduce the probability or the consequences of the identified risk, is based on the results of the prioritization. Risk assessment, on the other hand, usually deals with the analysis of a system with existing security measures and anticipates the weaknesses present in assessed system. However, these definitions are not generally accepted and sometimes each of these terms is used to describe a process that includes several of the other activities.

Although our search for articles specifically searched for articles about risk analysis or risk identification, the final list of selected articles contain some articles that mainly focus on risk management as a whole and some articles that focus only on one or more of the different sub-activities. Table 4 shows the focus of the selected articles within the field of risk management. It can be noticed that the majority of selected articles, 28 articles out of 57, are in fact about risk analysis. Further, it can be seen that 1 article is specifically about risk identification, 15 are about risk assessment, 1 is about risk prioritization, 2 are about risk mitigation and 20 are about risk management as a whole.

5.6 Qualitative and Quantitative risk analysis

Table 5 classifies the risk analysis methods in the selected articles as quantitative or qualitative. Quantitative methods express the probability and consequences of the identified risk as a numerical result. This makes it possible to calculate the relationship between loss prevention and cost associated with proposed countermeasures. Often it is difficult to use quantitative risk analysis because it is hard to estimate the exact probability and loss associated with each risk. Qualitative methods, on the other hand, use descriptive values such as ‘high’, ‘medium’ or ‘very low’ to express the probability and consequences of each risk. Both types of risk analysis methods are widely used for different types of systems, and in some cases they can be used together. Except for qualitative, quantitative and combined risk analysis methods, this study also identified semi-quantitative methods. This is an intermediary risk analysis technique that classifies the probability and consequences by using qualitative categories such as ‘financial loss between 10,000 USD and 100,000 USD’ or ‘less than once per 100 years’. It does not require the exact estimates needed for a quantitative risk analysis, but offers a more consistent approach than qualitative risk analysis. Not all of the selected articles contain enough information to determine whether a qualitative or quantitative approach was used, and for some articles the question is not applicable. Of the 38 articles that could be classified according to this criterion, 23 articles use a quantitative approach, 7 a qualitative approach, 6 contain a combined (quantitative and qualitative) risk analysis approach, and 2 are about semi-quantitative risk analysis methods.

6. DISCUSSION

First of all it can be observed that many of the identified articles have been published during the last few years before this study (2006-2011). This may mean that the amount of research has increased. As also discussed above, there may be other reasons, such as that the databases are more complete for later years. However, an increased dependence on information in the society, e.g. when critical processes to sensitive IT-systems. and in some cases they can be used together. Except for qualitative, quantitative and combined risk analysis methods, this study also identified semi-quantitative methods. This is an intermediary risk analysis technique that classifies the probability and consequences by using qualitative categories such as ‘financial loss between 10,000 USD and 100,000 USD’ or ‘less than once per 100 years’. It does not require the exact estimates needed for a quantitative risk analysis, but offers a more consistent approach than qualitative risk analysis. Not all of the selected articles contain enough information to determine whether a qualitative or quantitative approach was used, and for some articles the question is not applicable. Of the 38 articles that could be classified according to this criterion, 23 articles use a quantitative approach, 7 a qualitative approach, 6 contain a combined (quantitative and qualitative) risk analysis approach, and 2 are about semi-quantitative risk analysis methods.
Table 2: Focused systems in selected articles

<table>
<thead>
<tr>
<th>Type of System</th>
<th>articles</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT systems in general</td>
<td>1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 26, 27, 28, 29, 30, 31, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 52, 53, 54, 55, 56</td>
<td>49</td>
</tr>
<tr>
<td>Hospital systems</td>
<td>2, 32, 57</td>
<td>3</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>25, 50</td>
<td>2</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>E-government</td>
<td>51</td>
<td>1</td>
</tr>
<tr>
<td>Web-service systems</td>
<td>21</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 3: Type of research presented in selected articles

<table>
<thead>
<tr>
<th>Research type</th>
<th>Selected articles</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytical</td>
<td>1, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 29, 30, 31, 33, 37, 38, 40, 42, 43, 44, 45, 47, 48, 49, 50, 53</td>
<td>36</td>
</tr>
<tr>
<td>Empirical - Case study</td>
<td>2, 7, 15, 16, 17, 21, 26, 28, 32, 34, 36, 39, 41, 51, 52, 54, 55, 56, 57</td>
<td>21</td>
</tr>
</tbody>
</table>

Table 4: Focused risk management part in the selected articles

<table>
<thead>
<tr>
<th>Risk management part</th>
<th>Selected articles</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk analysis</td>
<td>1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 23, 24, 25, 26, 27, 29, 30, 32, 34, 35, 40, 42, 47, 50, 56, 57</td>
<td>28</td>
</tr>
<tr>
<td>Risk identification</td>
<td>32</td>
<td>1</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>5, 7, 9, 16, 31, 33, 36, 37, 39, 44, 45, 46, 52, 53, 55</td>
<td>15</td>
</tr>
<tr>
<td>Risk prioritization</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>Risk mitigation</td>
<td>12, 52</td>
<td>2</td>
</tr>
<tr>
<td>Risk management</td>
<td>1, 9, 10, 11, 17, 18, 19, 20, 21, 22, 27, 29, 30, 32, 35, 38, 43, 47, 48, 49</td>
<td>20</td>
</tr>
</tbody>
</table>

Table 5: Type of risk analysis method (quantitative or qualitative)

<table>
<thead>
<tr>
<th>Risk analysis type</th>
<th>Selected articles</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualitative</td>
<td>2, 12, 13, 14, 21, 34, 57</td>
<td>7</td>
</tr>
<tr>
<td>Quantitative</td>
<td>4, 5, 15, 19, 23, 24, 25, 26, 28, 31, 33, 36, 37, 39, 40, 41, 44, 49, 52, 53, 54, 55, 56</td>
<td>23</td>
</tr>
<tr>
<td>Combined approach</td>
<td>9, 10, 18, 42, 45, 46</td>
<td>6</td>
</tr>
<tr>
<td>Semi-Quantitative</td>
<td>3, 16</td>
<td>2</td>
</tr>
</tbody>
</table>
Table 6: Paper area vs. empirical or not

<table>
<thead>
<tr>
<th>Paper area</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>General</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Risk Analysis &amp; Assessment</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>Risk Analysis &amp; Management</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Risk Assessment &amp; management</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Risk Assessment &amp; mitigation</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Risk Assessment, prioritization,</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>and management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Identification, analysis,</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>and management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Risk Mitigation</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td><strong>SUM</strong></td>
<td>36</td>
<td>21</td>
</tr>
</tbody>
</table>

Table 7: Risk analysis approach vs. empirical or not

<table>
<thead>
<tr>
<th>Approach</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined approach</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>General</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>Qualitative</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Quantitative</td>
<td>13</td>
<td>10</td>
</tr>
<tr>
<td>Semi-quantitative</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>SUM</strong></td>
<td>36</td>
<td>21</td>
</tr>
</tbody>
</table>

Based on this mapping study of risk analysis methods for IT-systems discussed in the research literature, it can be concluded that most articles focus on new methods, and new frameworks and models for risk analysis. Only few papers focus on already available, and thereby maybe already known, methods. Further, it can be concluded that most research concerns general risk analysis methods, and not methods specific to certain types of IT systems.

The fact that only few articles focused on already available methods also means that it is not possible to say from the identified articles to what extent different methods are used in practice. For the same reason, it has not been possible to find many articles comparing available risk analysis methods, even if we argue that there is a need for this kind of research.

It can also be concluded that a majority of the identified articles present research that is non-empirical (36 articles), and fewer articles (21 articles) present case studies. None of the identified articles present research conducted as surveys or controlled experiments. Concerning what type of risk analysis methods that are presented in the published research, it can be concluded that most identified research concerns quantitative risk analysis methods.

Based on the findings a number of areas for further research can be identified. First of all it can be concluded that there is a need to conduct research where already available methods are investigated. This can for example be carried out as studies where different types of methods are compared in controlled experiments. We believe that methods for qualitative analysis are quite possible to investigate in controlled experiments [23], since they are possible to isolate from the whole management process to investigate them in a 'laboratory' setting. Having said that, we also believe that there is a need to further investigate the whole risk management process in longer case studies, where actual cases of risk management are investigated in practice.

ACKNOWLEDGEMENT

This work was funded by the Swedish Civil Contingencies Agency under a grant for PRIVAD, Programme for Risk and Vulnerability Analysis Development.

LIST OF SELECTED ARTICLES


(4) Bojanc, R., Jerman-Blazic, B., An economic modelling approach to information security risk management, In-


8. REFERENCES


