Applying the ENISA IT Risk Assessment for Cloud Computing on Small & Medium Enterprises.

A Case Study of Policy/Organizational, Technical and Legal Risks
1. Abstract

The IT risk assessment is a scientific and technologically based process consisting of three steps: risk identification, risk analysis and risk evaluation. A lot of IT risk assessments help the researchers, professionals and decision makers to identify the risks among those stands the ENISA (European Network for Information Security Agency) risk assessment. The risk assessment was specialized solely on Cloud Computing and that made it a perfect subject for examination in order to find out whether it holds strong and covers the necessary details in Cloud Computing when used by small enterprises. The research is a qualitative research with interpretive methodology. Through interviews it became easier and more efficient to conduct a close examination to help us understand and absorb the outcome of applying the ENISA risk assessment on small & medium enterprises. The research that was conducted has helped us spot the light on some of the important vulnerabilities for small enterprises and the reflections of the stakeholders on the risks and their ratings. The ENISA risk assessment provides a clear set of risks that assist and help enterprises cover Policy/Organizational, Technical and Legal aspects when using Cloud Computing technology and point out crucial vulnerabilities. The risk assessment is solid, clear, professional and reaches the satisfaction of stakeholders in small enterprises. Different reflections and outcome from applying the risk assessment could come as a result of the size of the enterprise and the stakeholders’ estimation for the business impact.

2. Keywords

ENISA risk assessment, cloud computing, cloud risk assessment, IT risks, vulnerabilities, policy & organizational risks, technical risks, legal risks
3. Introduction

Cloud Computing was introduced for the first time in the 1960s in the form of “Intergalactic Computer Network” by Professor J.C.R. Licklider (Mohamed, 2009). The idea was about networked computers serving several users (Pelkey, 2007). “It is a vision that sounds a lot like what we are calling Cloud Computing”, the explanation of Margaret Lewis product marketing director at AMD to the vision of J.C.R. Licklider (Mohamed, 2009).

Cloud computing refers today to applications and services that run on a distributed network using virtualized resources and accessed by common internet protocols and network standards. It is distinguished by the notion that resources are virtual and limitless and that details of the physical systems on which software runs are abstracted from the user (Sosinsky, 2011). Cloud Computing is increasing rapidly; Centaur Partners’ analysis of SaaS & cloud-based business application services revenue forecasts the market growing from $13.5B in 2011 to $32.8B in 2016 (Columbus, 2015).

From there comes the importance of IT risks assessment to identify and prioritize the risks not only to protect the Cloud Computing business investments, but to provide recommendations that maximize the protection of confidentiality, integrity and availability while still providing functionality and usability (SysAdmin, Audit, Networking, and Security, 2002). According to the European Network for Information Security Agency (ENISA) IT risk assessment is a scientific and technological process consisting of three steps: risk identification, risk analysis and risk evaluation (ENISA, 2005-2015).

According to Myndigheten för Samhällsskydd och Beredskap (MSB) conducting a Risk assessment is a very challenging process because according to the guidelines of it demands a team of experts and stakeholders with the right knowledge and experience add to that the time needed to conduct several meetings (MSB, 2011). The guidelines are not applicable for the Small and Medium Enterprise (SME), which are mostly limited by resources and time (Acs, Morck, Shaver & Yeung, 1997); There rises the importance to find a strong and capable risk assessment that help small enterprises detect the risks of using the cloud computing.

There are many frameworks, methods and risk assessments to help identify and prioritize the risks in IT systems like, e.g., Zachman, COBIT, ITIL, ENISA etc., most of them if not all focus on large enterprises; Information Technology Infrastructure Library (ITIL) has been widely used by big organizations like Microsoft, Fujitsu and Hewlett Packard (Azizi & Hashim, 2011). Researches that have been conducted before were focused mainly on conducting a risk management or assessing risks in the cloud computing (Dimitrov & Osman, 2014). In a study case in Switzerland, Brender and Markov (2013) have presented some main topics from a management point of view, those topics represents the specialists’ views regarding the major risks. In another study risks in outsourcing IT project in bank were identified as: 1) Based on the inside of the bank. 2) Based on outsourcing supplier. 3) Based on the external environment. (Yun, Xiaode & Yanyan, 2009).

After a long and careful search through internet research databases and corporations such as (IEEE Explore, Scopus) I found that none of the researches that were mentioned above or others have ever discussed the validity and the efficiency of a risk assessment in identifying the risks and the vulnerabilities in Cloud Computing for small enterprises; which is very important to help build the trust between small enterprises and cloud computing by identify the important risks to open the door for future research to improve the security of cloud computing,
furthermore it will help us identify a successful example of a risk assessment that can be used for future research purposes such as: compare with other risk assessments or build similar assessments with different scopes.

The challenge was to find a risk assessment that offers a list of prioritized and specified risks that help small enterprises assess and recognize the Cloud Computing IT related risks. We have decided to use the risk assessment presented by the European Network for Information Security Agency (ENISA, 2009) in a case study and explore whether it successfully covers the IT risks related to Cloud computing in a small enterprise or not.

4. Small and Medium Size Enterprises (SME)

SME stands for small and medium enterprises as defined in the European law: EU recommendation 2003/361. (European Commission, 2014). There are two major factors in determining the size of an enterprise: 1. Number of employees 2. Turnover or Balance sheet total.

Tabell 1 Categories of companies SME. (European Commission, 2014)

<table>
<thead>
<tr>
<th>Company category</th>
<th>Employees</th>
<th>Turnover</th>
<th>or</th>
<th>Balance sheet total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium-sized</td>
<td>&lt; 250</td>
<td>≤ € 50 m</td>
<td>≤ € 43 m</td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>&lt; 50</td>
<td>≤ € 10 m</td>
<td>≤ € 10 m</td>
<td></td>
</tr>
</tbody>
</table>

The three enterprises that we examined the risk assessment with them were small and medium size enterprises located in the city of Örebro in Sweden. The choice of companies from Sweden was important since Sweden is a member of the European Union and the ENISA risk assessment focuses mainly on SME in Europe. The first enterprise is small and is specialized in offering online services to customers around the globe through mobile application and a website. The enterprise has three departments: Administration, Communication & Marketing and Technical. The second enterprise is small also and is specialized in online marketing. It consists of three department: Management & Administration, Economy and Technical. The third enterprise is a medium enterprise specialized in system development, project management, technical support etc. with many departments: Administration, Economy, System Development, Technical Support, Business Development and Marketing & Sales. All companies have demanded a complete secrecy when interviewed due to the sensitivity of the subject.

5. Risk Assessment (ENISA)

Risk assessment by ENISA (2009) was made through several recommendations: building trust in the cloud, data protection in large scale cross-organizational systems and large scale computer systems engineering. In the process of creating the risk assessment the level of risks was estimated on the basis of the likelihood of an incident scenario, mapped against the estimated negative impact; by doing so the risks were given different ratings: low, medium and high. The risks in the risk assessment were categorized into three different scopes: Policy & organizational risks, Technical risks and Legal risks; which makes it easier to match the risks with the right stakeholders in order to make the right measures in terms of dealing with the risks. Each one of the risk categories includes a list of the risks detailed into (Probability level, Impact level, Reference to vulnerabilities, Reference to affected assets and Level of Risk). Beside risks the vulnerabilities are very important because of their nature.
A vulnerability is a security exposure that results from a product weakness that the product developer did not intend to introduce and should fix once it is discovered (Microsoft, 2015).

The ENISA risk assessment framework have three main pillars included in how a risk assessment should be performed.

1. Policy and organizational risks
2. Technical risks
3. Legal risks

In turn, these three main pillars have a number of predefined sub-risks. A complete list of these sub-risks can be found in appendix I.

6. Conceptual Framework
The conceptual framework was built based on the risk assessment of ENISA. The European Network for Information security Agency risk assessment has a list of risks divided into three categories: Policy & Organizational risks, Technical risks and Legal risks. Dividing the risks into three main categories will help us to control the process and examine the risk assessment as accurate as possible. Similar researches have taken the same approach such as (Saripalli & Walters, 2010) when they divided the threats into two major groups: Threat events compromising cloud security and Threat events compromising internet security. Each one of the risks is presented with vulnerabilities, probability, impact, affected assets and level of risk.

- Vulnerabilities: is a security exposure that results from a product weakness that the product developer did not intend to introduce and should fix once it is discovered.
- Probability: A risk is an event that may occur.
- Impact: A risk by its very nature, always has a negative impact.
- Affected assets: The assets that get affected by security exposure.
- Level of risk: the level of risk is estimated on the basis of the likelihood of an incident scenario, mapped against the estimated negative impact.

![ENISA Cloud Computing Risk Assessment Diagram](image-url)

*Figure 1. ENISA Risk Assessment Framework.*
7. Method

The method that was used in this research project was an interpretive methodology, with qualitative methods based mainly on interviews. The interpretive methodology seemed appropriate since the focus of the research is a study case (Andrade, 2009). The interviews were conducted on a one-to-one basis, once with the technical expert who is working in the IT system development department and another with the person responsible of or working in the administration department in the company.

The interviews were conducted separately for two main reasons: Each person will have the ability to focus on their specialist field, and to make sure that the respondents will not affect each other’s (Denscombe, 2010).

The interviews were unstructured, which means they were mainly about introducing the topic and letting the respondent steer the interview (Denscombe, 2010). The goal was to allow the interviewees to be more involved, lead the work sometimes and be more open to express their opinions.

The choice landed on the (ENISA, 2009) risk assessment for cloud computing and that’s for many reasons:

1. The presented ENISA risk assessment is concerned mainly by the Cloud-Computing risks.
2. The framework is presented for professionals and decision makers.
3. The risk assessment was prepared by experts from governments, organizations and major IT corporations which means it has a high sense of awareness and technological aspects (ENISA, 2009).
4. The ENISA works for the EU institutions and member states and is considered the EU’s response to the cyber security issues of the European Union (https://www.enisa.europa.eu/about-enisa).

The identified risks were classified into three categories: Policy & Organizational, Technical and Legal (ENISA, 2009). There is another set of risks which were not specified to the cloud and I have chosen not to include those risks in the research since the main focus in this study is the Cloud Computing.

Me as an interviewer I had the responsibility not only to present the risks mentioned in the ENISA risk assessment but also to explain the scopes of the risks and investigate the possibility of client dissatisfaction or missing risks and vulnerabilities. I have chosen to guide my interviews by an agenda (Minichiello et al., 1990; Briggs, 2000; McCann & Clark, 2005). An agenda is a broad guide to topical issues that might be covered in the interview, rather than the actual questions; it is open-ended and flexible (Burgess, 1984). My agenda consisted of a slide show to review the risks which were the main focus of the research. The interviews were conducted for two important reasons:

1. To review and explain the Risks and the (Vulnerabilities, Impact, Level of risk, probability and Affected assets) that were mentioned in the ENISA risk assessment in order to collect the reflections of the participants.
2. Brain Storming to figure out the risks that might were not considered by the ENISA risk assessment.
Early preparations and setting each interview to be up to 1 hour maximum are the most effective way of eliminating one of the challenges of this method which is it requires a significant amount of time to collect the needed information (Patton, 2002).

Recording the reflections and the opinions of the respondents during the interviews was through field notes which are the minimum requirements. The questions were asked and answers were recorded at the same time; since it was difficult to record everything at the time it was important to record again after the interview while the memory was still fresh in mind (Oates, 2006).

8. Data Analysis

The first interview was mainly conducted to introduce the risk assessment and the scopes of the risk categories in order to gain the approval of the stakeholders. The approval of the stakeholders is needed in order to keep the entire team in the same state of mind and focus their efforts on examining the ENISA risk assessment. The system and the challenges of the system when it is launched from the clouds were discussed in the second interview.

The interviews were divided later in three sessions: The two interviews with the head of the company have covered the Policy & Organizational and Legal risks while one interview with the system developer has covered the Technical risks. The questions were asked during the interviews and answers were gathered at the same time, in order to point their concerns, interests and satisfaction. Those segments were the most crucial elements in order to absorb the results and conclusions (Oates, 2006), since the research is about examining a risk assessment and see if it reaches the stakeholder satisfaction.

9. Results

In this section the results will be presented in ENISAs three main risk categories where the probability, impact, vulnerabilities, affected assets and level of risk will be detailed.

Tabell 2. Results of the interviews.

<table>
<thead>
<tr>
<th>Policy &amp; Organizational Risks</th>
<th>Probability</th>
<th>Impact</th>
<th>Vulnerabilities</th>
<th>Affected Assets</th>
<th>Level of Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Accepted without notes</td>
<td>Accepted without notes</td>
<td>Lack Of Resource Isolation, Lack Of Reputational Isolation, Cross-Cloud Applications Creating Hidden Dependency (technical), Storage Of Data In Multiple Jurisdictions And Lack Of Transparency About This, Lack Of Information On Jurisdictions, Lack Of Completeness And Transparency In Terms Of Use, Unclear Roles and Responsibilities, Lack Of Supplier Redundancy</td>
<td>Accepted without notes</td>
<td>Accepted without notes</td>
</tr>
</tbody>
</table>
## Technical Risks

<table>
<thead>
<tr>
<th>Risk</th>
<th>Notes</th>
<th>Communication Encryption Vulnerabilities, Lack Of Or Weak Encryption Of Archives And Data In Transit, Impossibility Of Processing Data In Encrypted Form, Key Generation: Low Entropy For Random Number Generation, Misconfiguration, System Or OS Vulnerabilities, Application Vulnerabilities Or Poor Patch Management, Inadequate Or Misconfigured Filtering Resources</th>
<th>Company’s reputation is missing from Risk 14, Insecure or ineffective deletion of data</th>
<th>Risk 8: Resource Exhaustion should be high</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accepted without notes</td>
<td>Accepted without notes</td>
<td>Accepted without notes</td>
<td>Accepted without notes</td>
<td></td>
</tr>
</tbody>
</table>

The stakeholders have stated when asked about their main interests are the risks within their expertise zone and whether there are certain risks they did not consider that should be managed in order to guaranty the safety of the data of their clients and at the same time protect the company on all aspects.

### 9.1 Policy & Organizational Risks

The stakeholder who was responsible for these risks stated when asked about his major concerns that the technical risks were far more important for the company than others. While all the risks were important to review and consider, yet still the technical were crucial in order to be able to guaranty the delivery of a well-functioning system worthy of customers trust. The second question about which is more important when analyzing the risks (Probabilities, Impact, Vulnerabilities, Affected Assets and level of Risk); it was important for the stakeholder to point the important aspect that helps the company choose the right Cloud services provider which was the vulnerabilities. The Affected Assets were also important to understand the amount of damage that might occur but the vulnerabilities were top priority.

The stakeholder awareness and understanding to the risks was for the most based on his knowledge of the Cloud computing technology so because of the fact that he did not have deep technical background, it was important to explain some of the risks to him.

The stakeholder comments were divided into Risks and vulnerabilities. Of the seven risks that were included in this category, two only were highlighted; the first risk is Risk.2 (Loss of Governance): in using cloud infrastructures, the client necessarily cedes control to the cp on a number of issues which may affect security. For example ToUs may prohibit port scans, vulnerability assessment and penetration testing. The second risk is Risk.7 (Supply Chain Failure): A cloud computing provider can outsource certain tasks of its production chain to third
parties. In such situation the level of security of the cloud provider may depend on the level of security of each one of the links and the level of dependency of the cloud provider on the third party. Both risks (2. and 7.) share one vulnerability which is vulnerability.22: Cross-cloud applications creating hidden dependency: hidden dependencies lies in the services supply chain (interior and exterior cloud dependencies) and the cloud services provider architecture does not support continued operation from the cloud when the third parties involved, subcontractors or the customer company, have been separated from the service provider and vice versa. This vulnerability was viewed by the stakeholder to be technical and should be viewed by the system developer.

The comments and thoughts has covered the vulnerabilities and the stakeholder has named the top vulnerabilities that the company must treat in order to guaranty a strong organization and cover all the flaws in the user policy to protect the company from user abuse or sabotage:

- **Vulnerabilities related to Cloud Computing:**
  1. Vulnerability.6 (Lack of Resource Isolation): the usage of resource by one customer can affect resource usage by another customer. IaaS cloud computing infrastructures rely mostly on designs where physical resources are shared by multiple virtual machines and therefore multiple customers.
  2. Vulnerability.7 (Lack of Reputational Isolation): activities of one customer could affect the reputation of another customer.
  3. Vulnerability.13 (Lack of Standard Technologies and Solutions): a lack of standards means that data may be ‘locked-in’ to a provider. This is a big risk should the provider cease operation that means disabling data altering.
  4. Vulnerability.22 (Cross-Cloud Applications Creating Hidden Dependency): Hidden dependencies exist in the services supply chain (interior and exterior cloud dependencies) and the cloud provider architecture does not support continued operation from the cloud when the third parties involved, subcontractors or the customer company, have been separated from the service provider and vice versa.
  5. Vulnerability.29 (Storage of Data in Multiple Jurisdictions and Lack of Transparency about this): mirroring data for delivery by edge networks and redundant storage without real-time information available to the customer of where the data is stored.
  6. Vulnerability.30 (Lack of Information on Jurisdictions): data could be stored and/or processed in jurisdictions where it is vulnerable to confiscation by force.
  7. Vulnerability.31 (Lack of Completeness and Transparency in Terms of Use): when usage policy is not clear and misses important issues.

- **Vulnerabilities which are not related to the Clouds:**
  1. Vulnerability.34 (Unclear Roles and Responsibilities): inadequate attribution of roles and responsibilities in the cloud provider organization.
  2. Vulnerability.47 (Lack of Supplier Redundancy): when Cloud service provider does not keep consistent performance.

Probability, Impact, Affected Assets and Level of Risks did not receive any remarks from the stakeholder and it reflects the accuracy of those four elements in the ENISA’s risk assessment.
When asked about whether if the risks have included all the possible vulnerabilities the stakeholder responded positively and mentioned that all the necessary vulnerabilities were highlighted and presented properly. The same answer was given when the question about if the risk assessment has covered all the risks related to Policy & Organization was introduced.

9.2 Technical Risks

The system developer who is responsible for the technical aspect have expressed genuine interest in the vulnerabilities and considered them as top priority when asked about the most important between (Probability, Impact, Vulnerabilities, Affected Assets and Level of Risk). He considered the vulnerabilities of a major importance to him since they point to the issues that he needs to manage in order to improve the security of the system. The Affected Assets and Level of Risk were also interesting but not as important as the vulnerabilities.

The majority of the risks were clear and easy to understand by the system developer but he needed some help understand few risks, the ability to understand the risks was based on the amount of knowledge of the system developer and how engaged he was in his technical field.

The system developer highlighted three risks between thirteen technical risks when asked about his comments and thoughts. Risk 8. (Resource Exhaustion – under or over provisioning) which is the case of service not functioning because it is entirely consumed.

The affected assets don’t include the company’s reputation (A1) which is considered by the system developer to be the asset that get affected the most by the risk. It is damaging to the company if the clients think it is inadequate to perform a certain important function.

Risk 14. (Insecure or Ineffective Deletion of Data) this occurs when a request to delete a resource in the cloud doesn’t result with the data fully wiped because of certain procedures.

Risk 20. (Conflicts between Customer Hardening Procedures and Cloud Environment). This is the result of cloud customers not protecting their environment at the same time the cloud provider did not take the right steps for isolation.

This risk is considered by the expert to be more Administrative than technical since the main threat comes from cloud providers which demands an administrative control over the requirements that need to be clarified when choosing a cloud provider.

The comments of the system developer have extended to cover the vulnerabilities and he pointed out the crucial vulnerabilities that need to be covered and treated properly. There were a set of vulnerabilities under each risk but only the crucial ones were pointed for further consideration and they were divided into Vulnerabilities related to Cloud computing and non-related:

- **Vulnerabilities Related To Cloud Computing**

1. Vulnerability.8 (Communication Encryption Vulnerabilities): which concern the possibility of reading data in transit via, for example; MTM attacks, poor authentication, acceptance of self-signed certificates, etc.

2. Vulnerability.9 (Lack Of or Weak Encryption Of Archives And Data In Transit): the failure to encrypt data in transit, data held in archives and databases, un-mounted virtual
machine images, forensic images and data, sensitive logs and other data at rest puts the data at risk.

3. Vulnerability.10 (Impossibility of Processing Data in Encrypted Form): Encrypting data at rest is not difficult but despite recent advances in homomorphic encryption, there is little prospect of any commercial system being able to maintain this encryption during processing.

4. Vulnerability.12 (Key Generation: Low Entropy For Random Number Generation): the combination of standard system images, virtualization technologies and a lack of input devices means that systems have much less entropy than physical RNGs.

- **Vulnerabilities not related to the clouds:**

  1. Vulnerability.38 (Misconfiguration): inadequate application of security baseline and hardening procedures, human error and untrained administrator.

  2. Vulnerability.39 (System or OS vulnerabilities): when the running system has defects or errors when released to the market.

  3. Vulnerability.48 (Application vulnerabilities or Poor Patch Management) include: bugs in the application code, conflicting patching procedures between provider and customer, application of untested patches, vulnerabilities in browsers, etc.

  4. Vulnerability.53 (Inadequate or Misconfigured Filtering Resources).

Neither Probability nor Impact had any remarks from the system developer which points out the accuracy of these aspects in ENISA’s risk assessment.

The system developer has stated that the risk assessment has successfully covered all the vulnerabilities and the affected assets and even more. He also mentioned that the risk assessment has included all the technical risks that concerned him. It is worth mentioning that the high quality of cloud computing services provided by the service provider has played a major role in minimizing, eliminating or accepting the technical risks. There were 13 major risks identified in the technical risk category in the risk assessment but only three risks were highlighted by the company.

The other ten risks were not highlighted because they were not considered as a priority by the company. The risks were mostly in the zone of the cloud computing service provider which made them important to consider and reviewed but not necessarily prioritized since they are out of the reach of the company.

### 9.3 Legal Risks

The main concern of the stakeholder is represented in two: First, learn about the legal risks as an educative tool that helps identify the complexity of the Cloud computing in order to be able to point the responsibilities and juridical complications of both the company and the Cloud service provider. Second, use the highlighted juridical issues to help include them in policy contracts that go to future clients. In respond to the second question about which element is more important the answer given by the stakeholder was that both vulnerabilities and affected assets have almost the same importance. The vulnerabilities helped the company identify the weaknesses and the affected assets helped them understand some of the issues that the company needs to specify the responsibility of all parts in cloud computing (Service Provider, Service Manager (company) and Service User (online users)).
The risks for the biggest part were clear but like the risks in the first two categories, further explanation was needed to explain some risks. After going through the risks and explaining them only one remark was made by the stakeholder about level of risk in Risk.24: (Licensing Risks). The stakeholder thought that the risk does not elevate to the level of importance that was given to it since it was covered systematically by arranging licenses with all the involved parts (license to develop the system, license to develop the app, license to the platform, etc.).

The stakeholder has stated that the legal risks has included all the vulnerabilities and affected assets; furthermore all the risks have covered the legal aspect successfully.

10. Discussions

For the small enterprises the Technical vulnerabilities were far more important to handle and control than Policy & Organizational and Legal. The reason behind it is that Organizational vulnerabilities were more like something to consider as part of future plan in case the small enterprise expanded while Technical vulnerabilities are more about the current state of the enterprise and help support and protect the IS system and the company. Vulnerability evaluation should be conducted and its results should be available to potential users (Matsumoto, 2002).

For small enterprises the organizational risks are not very threatening since the hierarchy in small enterprises is very clear and easy to manage due to the fact that the number of employees is small. However Policy & Organizational and Legal risks are eye opening risk categories for small enterprises owners and project managers to the administrational and legal challenges and the requirements that need to be considered and thought.

11. Conclusion

Purpose of the research was to examine a cloud computing risk assessment for small enterprises in order to determine its efficiency and reliability; that risk assessment was conducted by the European Network for Information Security Agency. When conducting a study case in a company one expects a collision between the academic world and the business world. A challenge that was managed smoothly which points a very important and successful element in the ENISA risk assessment. The risk assessment has named three major categories for the IT risks which are Technical, Organizational & Policy and Legal. Each one of these categories has included a list of risks with (Probabilities, Impact, Vulnerabilities, Affected assets and Level of Risk) and they were accepted and very well received by the stakeholders of the small enterprise where the risk assessment has been tested. The stakeholders have expressed their satisfaction and they were pleased by the ENISA risk assessment which has provided them with a clear list of detailed risks that after careful examination has successfully identified and covered many risks in Cloud Computing. The stakeholders have also reached a level of comfort and understanding to what can be improved or accepted. The main interest of the stakeholders was focused on the vulnerabilities because it represented an extension which needs more investigation in order to either find solutions, minimize the risk or to reach a level of risk acceptance. The stakeholders made comments on the other components of the risks (Level of risk, Impact, Probability, Affected assets) but they did not consider them as real major issues. The ENISA risk assessment is a good and strong risk assessment that successfully points out most of the risks and vulnerabilities for small enterprises. Understanding the IT risks was a major factor in the stakeholders coming to term with reality and accept the situation at the same time it made them aware of the demands that must be delivered by the service provider. One
very important aspect I can recall from applying risk assessment to small enterprises is that the people who are concerned by the process (Stakeholders like owners or workers) are not only interested about risks but about exploring new areas they haven’t think that could require self-awareness or improvement.

12. Future work
As I went through the details of the Cloud computing and the risk assessment it became obvious that Cloud Computing risks can be categorized into different scopes. The stakeholders are most curious and interested in the risks they can treat (minimize/terminate). For future research it would be very useful and interesting to see a risk assessment based on categorizing risks into Cloud Computing service provider risks and Cloud Computing client risks. Such risk assessment could help very much by pointing out the risks and the vulnerabilities that could be treated by the Clients and the risks that can be treated by the service providers. A further research in improving the level of cloud computing based on client recommendations could be very interesting.

13. Acknowledgment
Thanks and appreciations to persons who influenced my study and supported me with their knowledge and experience.

Karin Winberg
Intern revision manager at Kommuninvest i Sverige AB
Fredrik Karlsson
Professor in informatics at the University of Örebro
Sirajul Islam
Assistant professor in informatics at the University of Örebro
Emil Carlsson
Information Student in the University of Örebro
Johannes Sahlin
Information Student in the University of Örebro
14. References


15. Appendix

- Interview questions:

1. What are your main concerns?
2. Here are the risks; what is more important for you (Probabilities, Impact, Vulnerabilities, Affected assets and Level of Risk)?
3. Do you understand the risks?
4. What are your comments and thoughts about the risks? (Probabilities, Impact, Vulnerabilities, Affected assets and Level of Risk).
5. Based on the previous question; Do you think the risks have included all the related vulnerabilities, Affected Assets?
6. Do you think the mentioned risks cover all your concerns?