2010

A Collaborative Process Based Risk Analysis for Information Security Management Systems

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Sevgi Ozkan
Middle East Technical University

Recommended Citation

Karabacak, B., & Ozkan, S. (2010). A Collaborative Process Based Risk Analysis for Information Security Management Systems. *The Proceedings of the 5th International Conference on Information Warfare and Security* Retrieved from https://fuse.franklin.edu/facstaff-pub/41

A Collaborative Process Based Risk Analysis for Information Security Management Systems

Bilge Karabacak[1] and Sevgi Ozkan[2]
[1]TUBITAK, Ankara, Turkey
[2]METU, Ankara, Turkey
sozkan@ii.metu.edu.tr
bilge@uekae.tubitak.gov.tr

Abstract: Today, many organizations quote intent for ISO/IEC 27001:2005 certification. Also, some organizations are en route to certification or already certified. Certification process requires performing a risk analysis in the specified scope. Risk analysis is a challenging process especially when the topic is information security. Today, a number of methods and tools are available for information security risk analysis. The hard task is to use the best fit for the certification. In this work we have proposed a process based risk analysis method which is suitable for ISO/IEC 27001:2005 certifications. Our risk analysis method allows the participation of staff to the determination of the scope and provides a good fit for the certification process. The proposed method has been conducted for an organization and the results of the applications are shared with the audience. The proposed collaborative risk analysis method allows for the participation of staff and managers while still being manageable in a timely manner to uncover crucial information security risks.

Keywords: ISO/IEC 27001:2005, information security, risk analysis, flow chart, process approach

1. Introduction

Recently, companies have been showing a wide interest in ISO/IEC 27001:2005 (ISOa 2005) and ISO/IEC 27002:2005 (ISOb 2005) standards. The existence of ISO/IEC 27001:2005 certification has been the main interest. It has been proposed that ISO/IEC 27001:2005 certification will be widely accepted by companies in the near future. Today, many organizations quote intent for ISO/IEC 27001:2005 certification. While some organizations are en route to certification, some of them are already certified (CSF 2003).

ISO/IEC 27001:2005 provides a model for setting up and managing an effective Information Security Management System (ISMS). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. Thus, the most crucial step to fulfill these requirements is to perform a risk analysis with respect to business risks. ISO/IEC 27001:2005 does not recommend a specific risk analysis method; rather it just states it to be a mandatory process by the requirement to "define a systematic approach to risk assessment" (ISOb 2005).

ISO/IEC 27001:2005 mandates the process approach for the whole course of action. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. The design and implementation of an organization's ISMS is influenced by the processes within the organization (ISOb 2005). While applying ISO/IEC 27001:2005, a process approach should be followed, thus, the application of a system of processes, identification and interaction of these processes and their management should be analyzed successfully.

As mentioned previously, risk analysis is a vital part of establishing ISMS, thus a process approach should be applied to the risk analysis method as well. The risk analysis methods that do not have a process approach do not fit well into ISO 27001 certification processes.

In this work, we have proposed a paper based, qualitative and collaborative risk analysis method by taking the requirements of the ISO/IEC 27001:2005 into consideration. The proposed risk evaluation method has been applied in a real organization. The organization has been pursuing ISO/IEC 27001:2005 certification. Because the proposed risk analysis method fulfills the requirements that are stated in the standard, it is especially designed for companies that pursue ISO/IEC 27001:2005 certification. In this paper, not only a novel risk analysis method is described but also the results of its application are presented briefly.

This paper is organized as follows: The challenges of risk analysis for information security and risk analysis methods for information security are introduced briefly after the Introduction. The risk model and application details of the method is presented afterwards. The next section contains some ideas on the verification, comparison and the results of the application. The last section is the conclusion.

2. Risk analysis methods for information security

Generally, risk analysis is a rather complicated process because the risks are based on probability. The complexity of the risk analysis process has become much more pronounced when information and communication technologies became widely used. In terms of information technologies, risk is not a simple probabilistic value. It is the probability of a threat successfully attacking an asset via a particular vulnerability. Thus, risk depends on three inputs, asset, vulnerability and threat.

$$\text{Risk} = \boldsymbol{f}\,(\text{Asset, Vulnerability, Threat})\ . \qquad (1)$$

Function f given in the formula (1) shows an abstract risk model, it has three inputs and the output; risk.

There are some other reasons for the particular complexity of information security risk analysis. First of all, information is one of the most fundamental and important assets for companies. Thus, peculiar attention should be given to information assets while performing risk analysis. However, information is an abstract asset. Information can exist in many forms, electronic, hard copy, verbal etc. Information does not have the capability of protecting itself against malicious actions. Information is not the only asset for companies in terms of information security. Hardware, software, storage media, humans and hardcopy documents are assets as well. Another reason for the difficulty of information security risk analysis is the correlations between these asset categories. Vulnerability in an asset may turn into a threat for the other assets. As an example, a computer virus may use the vulnerability of outdated computer virus database. However, information, software, humans and company reputation may suffer from computer viruses. Reputation is just another abstract asset like information. Its value cannot be measured in monetary terms. Risk analysis methods for information security would need to answer all of these challenges.

There are a number of information security risk analysis methods available today. It is better to bring a systematic approach to examine these methods. There are two types of risk analysis methods in terms of content. Quantitative risk analysis methods contain mathematical instruments to evaluate risk. Qualitative risk analysis methods do not contain any mathematical instruments. There is also another classification for risk analysis methods based on the application methodology. Paper based risk analysis methods do not use any specialized software in the process. All of the work is done by paperwork or by using a simple spreadsheet software, there are a number of risk analysis software available in the market. Four basic risk analysis methods come forth by combining these two classification schemes. These are paper based and quantitative, paper based and qualitative, software based and quantitative and finally software based and qualitative. There are examples from academia or industry for each of these risk analysis categories (Karabacak 2005).

There are a lot of software tools which help perform risk analysis. Some of them have specific risk model. CRAMM and RiskWatch are the most popular software tools, which are based on quantitative peculiar risk models (Karabacak 2006). They are compliant with the risk analysis requirements of ISO/IEC 27001:2005. Cobra is a qualitative risk analysis software, which is based on questionnaires (Karabacak 2006). Using software in risk analysis methods may have some disadvantages. First, the cost of such methods is usually high. Second, the main frame of the risk analysis process is drawn by the software. Thus, some necessary variations of the risk analysis process would not be achieved (Karabacak 2005). The second factor is an important disadvantage when the software is not specifically designed for ISO/IEC 27001:2005 certification.

Some of the quantitative tools, which can be used in a risk analysis process, use complex mathematical tools like Bayesian networks, fuzzy logic, simulation and fault trees (Aven 1998, Ru 1996, Staker 1999, Bilbao 1992). These mathematical tools are advanced and comprehensive instruments in order to model specific risk situations in depth. As an example, Ru and Eloff shows the modeling of the possible exploitation of vulnerabilities associated with a hard disk drive and a customer database contained on this hard disk drive by using Fuzzy logic (Ru 1996). Staker says that different types of asset will have different risk models by using Bayes Nets (Staker 1999). This requirement may make the execution of a risk analysis process difficult. Bilbao shows the risk models of three situations; hold up, burglary and vandalism, as sample risk models in his paper (Bilbao 1992). The calculations of these three examples take a lot of place as shown in Bilbao's paper. As a result, although complex mathematical methods may model specific situations comprehensively and accurately, they may require tremendous mathematical calculation to be fit into the information security area that spans wide risk scenarios.

ISRAM is an example of paper based quantitative risk analysis methods. ISRAM is basically a survey preparation, conduction and analysis method specialized for information security (Karabacak 2005). ISRAM can be used in the risk analysis process for ISO/IEC 27001:2005 certification. But performing the whole risk analysis process only by using ISRAM will not be suitable for two reasons. Firstly, ISRAM does not satisfy some of the requirements of ISO/IEC 27001:2005, such as asset valuation. Secondly, it may take a long time to prepare and conduct the survey for the whole process. However, ISRAM can successfully be used in some parts of the whole process. ISRAM has also been used in risk analysis applications. It helps to obtain staff opinions of the organizations effectively.

Risk analysis methods for ISO/IEC 27001:2005 certification should have the capability of determining the scope, the processes within this scope, the interrelationships of the processes, the assets within the processes, the vulnerabilities of the assets, the threats and finally the risk. The methods that have heavy quantitative tools may fail during the modeling process. Not all of the software supports the schema of ISO/IEC 27001:2005 risk analyses. There are tools that support ISO/IEC 27001:2005 like CRAMM and RiskWatch, but not all organizations may afford software like these. In this paper, we proposed a paper-based and qualitative risk analysis method, which has these capabilities using a collaborative process approach. This method does not contain elaborate mathematical instruments that complicate the modeling and is a cost-effective method for companies.

3. Process based risk analysis method

In the proposed method, information security risks are evaluated after defining the processes. Specific examples are given for each process from the case study. The workflow of our risk analysis process is given in Figure 1. The subsections in this section are based on the steps depicted in Figure 1. Thus, by following the subsections, the entire risk analysis process is covered. First and second steps are mandatory for ISO/IEC 27001:2005 certification. The steps from three to five are done to provide useful and required inputs for the core risk analysis process, the dashed line in Figure 1.

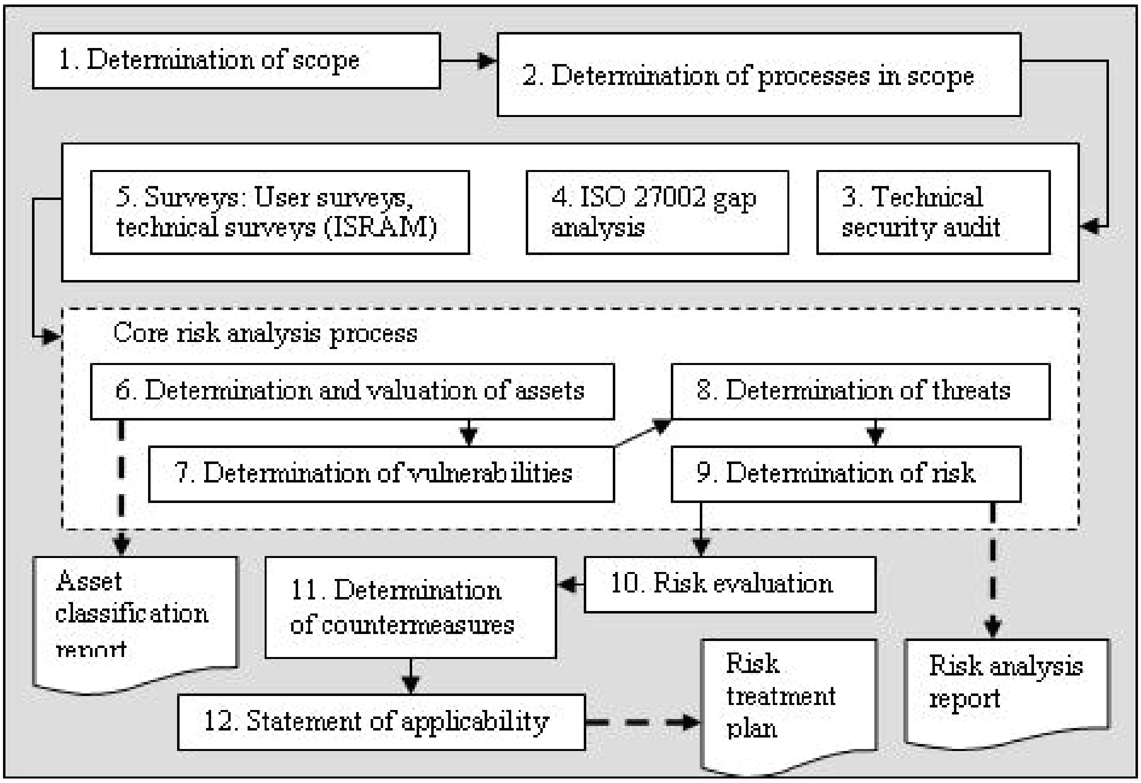
1. Determination of scope
2. Determination of processes in scope
5. Surveys: User surveys, technical surveys (ISRAM)
4. ISO 27002 gap analysis
3. Technical security audit
Core risk analysis process
6. Determination and valuation of assets
8. Determination of threats
7. Determination of vulnerabilities
9. Determination of risk
Asset classification report
11. Determination of countermeasures
10. Risk evaluation
Risk treatment plan
Risk analysis report
12. Statement of applicability

Figure 1: Overall structure of proposed method

3.1 Determination of the scope

Scope is the area that the risks are identified. The determination of scope is a requirement of ISO/IEC 27001:2005. As an ISO/IEC 27001:2005 term, the organization will need to present its scope for a proposed Information Security Management System to the requirements of ISO/IEC 27001:2005 (ISOb 2005). The scope defines the activities, functions and services to be provided to internal and / or external customers. Thus, scope draws the frame of the risk analysis.

3.2 Processes determination

After the determination of the scope, the process that exists within the scope is determined. A process is an organized set of activities which transforms inputs into outputs. A process can be seen as a value chain by contributing to the creation or delivery of a product or service. The processes that are determined in our study are network, substructure, security, terminal, storage, backup and database processes.

3.3 Technical security audit

What is done in this step is to determine the vulnerabilities of the assets in the processes. This task is done by using vulnerability scanners with the guide of predefined test procedures. The result of the audit is an important and useful input for determining vulnerabilities of assets, vulnerability levels and impact level / likelihood of threats, which are determined within the core risk analysis process.

At the beginning of technical security audits, the assets within the processes are listed. All of the assets within the processes are tested by using scripts, specialized scanners and by the guidance of the test procedures. All of the results of technical security audits are documented and saved to be used in the subsequent steps of the process.

3.4 ISO 27002 gap analysis

This step compares organization’s overall security posture to those identified and accepted by ISO/IEC 27002:2005. Gap analysis is used to identify the divergence of existing security controls against the standard. It provides comparative analysis. Thus, organization’s current level of compliance is measured. Like the technical security audit, gap analysis helps determining the vulnerability levels at various security domains in the standard like physical security and personal security. It is important to note that the scope should not be ignored during this step. All of the findings are documented to be used in the core risk analysis process.

3.5 Surveys

The goal of the surveys is to try to understand the security awareness level of employees within the scope and to learn some technical details about the assets within the processes.

Standard employee surveys and technical surveys are conducted to reach these purposes. Employee surveys are for the purpose of estimating the security awareness level within the organization. Technical surveys are prepared for each of the processes in the scope and expected to be answered by process operators. Thus, seven technical surveys are prepared in our case study.

For the employee survey, ISRAM is used. By using ISRAM, preparation, conduction and evaluation of the surveys are performed structurally and systematically. The level of security awareness of employees within the scope came out as 3 out of 5, which is a medium level of awareness. Security awareness raising activities were recommended for this organization.

Surveys have an important value for risk analysis. They allow participation of the employees to the risk analysis process directly. All of the surveys which are distributed to employees are collected back and stored to be used in the core risk analysis process.

3.6 Determination and valuation of assets

This step is the starting point of the core risk analysis process. The results from the previous steps are used in the subsequent steps including this step. This situation is depicted in Figure 1.

During the determination of assets within the scope, it is important to take into account whether or not the specified asset's absence has an impact on confidentiality, integrity or availability. If it has an impact, then the asset is written in a spreadsheet to be evaluated in further risk analysis steps. The results of the technical survey are used in this step.

Two independent asset valuation criteria are used in our risk analysis method. The first one determines the impact of the abuse of the asset on confidentiality, integrity and availability. The other criterion is the total monetary loss, when the asset is abused. Because of the space limitations, the template, Table 1, is shown for the first criterion. For the second criterion, Table 2 is used. It can be said that, Table 1 is qualitative and Table 2 is quantitative.

Table 1: The reference table for confidentiality, integrity, availability (template)

	Confidentiality	Integrity	Availability
Low	When the asset is abused, no critical information is exposed. The exposed information, which is not critical, does not affect the organization adversely, or has little impact on the organization.	When the asset is abused, critical information is not altered . Altered information, which is not critical, does not affect the organization adversely, or has little impact on organization.	When the asset is abused, critical information will still be available. The uncritical information, which becomes unavailable, does not affect the organization adversely, or has little impact on organization.
Medium	When the asset is abused, no critical information is exposed. The exposed information, which is not critical, affects the organization. The adverse effect may be compensated in the medium term.	When the asset is abused, critical information is not altered . Altered information, which is not critical, affects the organization. The adverse effect may be compensated in the medium term.	When the asset is abused, critical information will still be available. The uncritical information, which becomes unavailable, affects the organization. The adverse effect may be compensated in the medium term.
High	When the asset is abused, critical information is exposed. The exposed information affects the organization adversely. The adverse effect may be compensated in the medium term.	When the asset is abused, critical information is altered . The altered information affects the organization adversely. The adverse effect may be compensated in the medium term.	When the asset is abused, critical information will not be available. Unavailable critical information affects the organization adversely. The adverse effect may be compensated in the medium term.
Very High	When the asset is abused, critical information is exposed. The exposed information affects the organization adversely. The adverse effect may not be compensated or may be compensated in the long term.	When the asset is abused, critical information is altered . The altered information affects the organization adversely. The adverse effect may be compensated in the long term.	When the asset is abused, critical information will not be available. Unavailable critical information affects the organization adversely. The adverse effect may not be compensated or may be compensated in the long term.

The value of an asset is assessed by taking the total monetary cost into consideration, when the asset is abused. For instance; when the backbone switch is damaged, both the cost of the switch and the cost of unavailable business activities during interruption should be considered. The value of an asset is totally independent from the confidentiality, integrity and availability values. One asset may affect the confidentiality and integrity very high, but its value may be low.

Table 2: The reference table for the monetary value

Low	The abuse of asset costs minor consequences.
Medium	The abuse of asset costs less than 5K USD.
High	The abuse of asset costs between 5K USD and 10K USD.
Very High	The abuse of asset costs more than 10K USD.

The total monetary costs and discretisations, which are shown at Table 2, were determined by holding a meeting with the representatives of the organization. Because, it is not a large scale organization, it was agreed that the values were suitable for the organization.

All of these tables are dynamic in content. For example, the monetary values in Table 2 can be changed according to the budget of the organization. Also, the security requirements of the company could change the contents of Tables 1 and 2.

All of the results of asset determination and asset valuation processes are written on spreadsheets and an asset classification report is produced. In Table 3, the template of asset classification and evaluation documentation is shown.

Table 3: Asset classification and valuation template

Asset	Description	Belonging Process	Owner	Confidentiality	Integrity	Availability	Value

3.7 Vulnerability and threat analysis, risk analysis

The next three steps are explained in the same section, because the steps are strongly related with each other. What is done in these steps is as follows;

Firstly, the vulnerabilities of assets within each process are listed. The results of technical security audit, ISO 27002 gap analysis and surveys are used.

The threats which may exploit these vulnerabilities are determined and listed. By taking the values of assets, the criticality of vulnerabilities, the strengths of already used countermeasures and the nature of threats into consideration, the likelihoods and impact levels of threats are determined. Again, the main information sources for these parameters are process models, technical audits, gap analysis and surveys.

The reference table for the likelihood of the threat is given in Table 4. The reference table for the impact level of the threat is given in Table 5. There is no reference table for the vulnerability level and the protection level of the countermeasures at present. But these parameters were considered during the determination of the risk.

Table 4: The reference table for the likelihood of threats

Low	< = once per year
Medium	< = once every six months
High	< = once per month
Very High	= > once per day

Table 5: The reference table for the impact level of threats

Damage may be compensated …	Threat Prevalence		
	Department	Organization	Organization and business partners
… in the short term.	Low	Medium	High
… in the short/medium term.	Medium	High	High
… in the medium term.	High	High	Very High
… in the long term (or damage may not be compensated)	High	Very High	Very High

The abstract risk model for determining the risk level is shown in Formula 2 (NIST 2001), (McEvoy 2002), (USGAO 1999). These parameters directly contribute to risk value. Also, these parameters are placed at the rows and the columns of Table 6, the reference table for the value of risk. The other parameters like asset value, vulnerability level are implicit parameters. These parameters change the levels of explicit parameters, hence they change the risk.

$$\text{Risk} = \text{likelihood of threat} * \text{the impact level of threat} \qquad (2)$$

The contents of Table 6 may be changed in order to reflect the specific security requirements of the organization.

Table 6: The reference table for the value of risk

Risk = The likelihood of threat * The impact level of threat		The impact level of threat			
		L	M	H	VH
The likelihood of threat	L	L	L, M	M	M, H
	M	L, M	M	M, H	H
	H	M	M, H	H	H, VH
	VH	M, H	H	H, VH	VH

All of the results of likelihood and impact level determinations are written in spreadsheets and a final risk analysis report is produced. In Table 7, the template of risk analysis documentation is shown.

Table 7: Risk analysis template

Asset	Vulnerability	Threat	Impact	Likelihood	Risk	Risk Description

3.8 Risk evaluation

The risk values that are determined by the risk analysis process are unrefined and raw risk results for the organization. The risk results of risk analysis are not useful alone. These risk results need to be assessed according to the predefined criteria of organization. After assessing the risks, they should be prioritized. The criteria that need to be considered during risk evaluation process are the security requirements of organization, the cost of countermeasures, the budget of organization and the usability and the operability of the countermeasure. All of these evaluation processes are performed with the participation of employees of the organization.

Risk evaluation process starts with determining the degree of assurances. Degree of assurance is the process of identifying the acceptable levels of risks. In other words, it is how much protection we expect from the countermeasure for a specified risk. The degree of assurance reflects the security requirements of the organization. By taking all of the criteria into account, risk prioritization is performed. Risk prioritization is the order the countermeasures should be applied. Risk prioritization is done by using Table 8.

Table 8: Risk prioritization method

Priority		Importance			
		L	M	H	VH
Cost	L	L, M	M	H	VH
	M	L	M	M, H	H, VH
	H	L, negligible	L, M	M, H	H, VH
	VH	Negligible	L	H	H, VH

There are two fundamental explicit inputs for determining priority: the cost of the countermeasure and the importance of the countermeasure. The importance is determined by taking the bulk risk level and the degree of assurance into account. The cost includes the price of the planned countermeasure and the operation and its setup costs. The budget of the organization also contributes to this value. Priority level is determined by assessing these parameters according to Table 8. It should be noted that, the usability and the operability of the countermeasure should not be circumvented. The contents of Table 8 are particular to the structure of the organization, thus its content can be changed to reflect the organization's needs.

Risk evaluation stands between risk analysis and risk treatment. After risks are prioritized, determination of countermeasures is performed.

3.9 Countermeasure determination

Like other steps, countermeasure determination is performed with the participation of the organization staff. While determining countermeasures, the priorities determined during the previous step are considered.

The crucial output of this step is the risk treatment plan. Risk treatment plan is an organized calendar in which the countermeasures and their implementation details exist.

All of the results of the likelihood and impact level determinations are written in spreadsheets and a final risk analysis report is produced. The details of risk evaluation and risk treatment steps are documented. In Table 9, the template of the risk evaluation and countermeasure determination documentation is shown.

Because the risk level is decreased or the risk is eliminated by using countermeasures, countermeasures selection is one of the most crucial steps of the establishment process of ISMS. Security countermeasures may be made for formulating an effective overall security solution to address threats at all layers of the information infrastructure (Kim 2005). Kim and Lee propose a method for the selection of countermeasures. In this method, information value, threat level, security services, the scope of security services are considered for selection of both technical and non-technical countermeasures. In our case study, the same factors were taken into consideration for the selection of countermeasures. ISO 27002 is a vital source for countermeasure determination and selection (ISOb 2005). This standard has 133 high level countermeasures that cover both internal and external threats. Yeh and Chang also emphasize the importance of this standard (Yeh 2007). Except for externally requested regulations, such as privacy laws or government regulations, firms mostly determine their security policies and procedures internally (Yeh 2007). During our case study, ISO 27002 was an important source that is used for the selection of countermeasures. The selection process took up much time compared with the other steps of case study; during this process both the staff of the organization and the consultants as external factors studied.

Table 9: Risk evaluation and countermeasure selection template

Column1: Asset	Column2: Vulnerability	Column3: Risk Description	Column4: Risk Level	Column5: Degree of Assurance

Column6: Countermeasure Suggestion	Column7: Importance	Column8: Cost	Column9: Priority	Column10: Result

4. Verification, comparison and the results of the application

In this section, some brief information on the organization's information technology infrastructure is conveyed. A visual technical presentation of the system is given in Figure 2.The information system carries all the business processes of the organization. This information system is operated by five administrators.

Information security was not considered systematically in the design of this system like the PACS (Tong 2003)

The result of the risk analysis process for this information system is shown briefly in Table 10. A total amount of 115 risks are found in all of the processes within the scope. As shown in Figure 3, three percent of these risks are very high. The majority of the risks are high, medium and low level risks

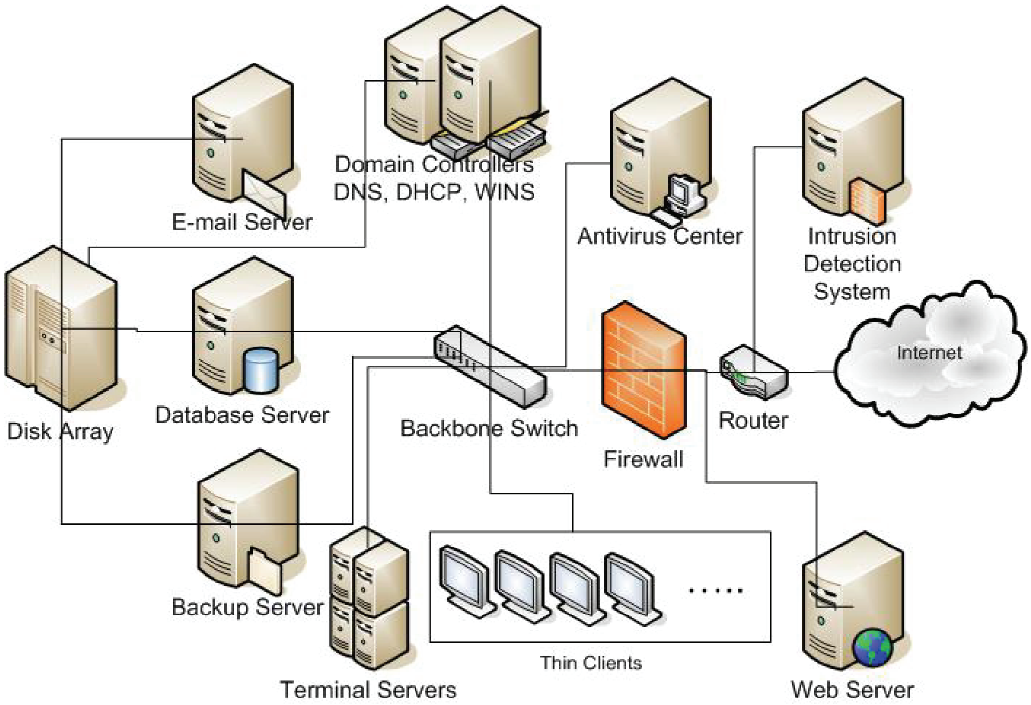

Figure 2: The information system of the organization

Table 10: Risk distribution table

	The risks				
Process	Very High	High	Medium	Low	Total number of risks
Network Process	0	11	15	8	34
Substructure Process	2	10	10	9	31
Security Process	0	3	4	5	12
Storage Process	0	7	2	2	11
Terminal Process	0	1	1	3	5
Database Process	1	9	2	0	12
Backup Process	0	0	6	4	10
Total	3	41	40	31	115

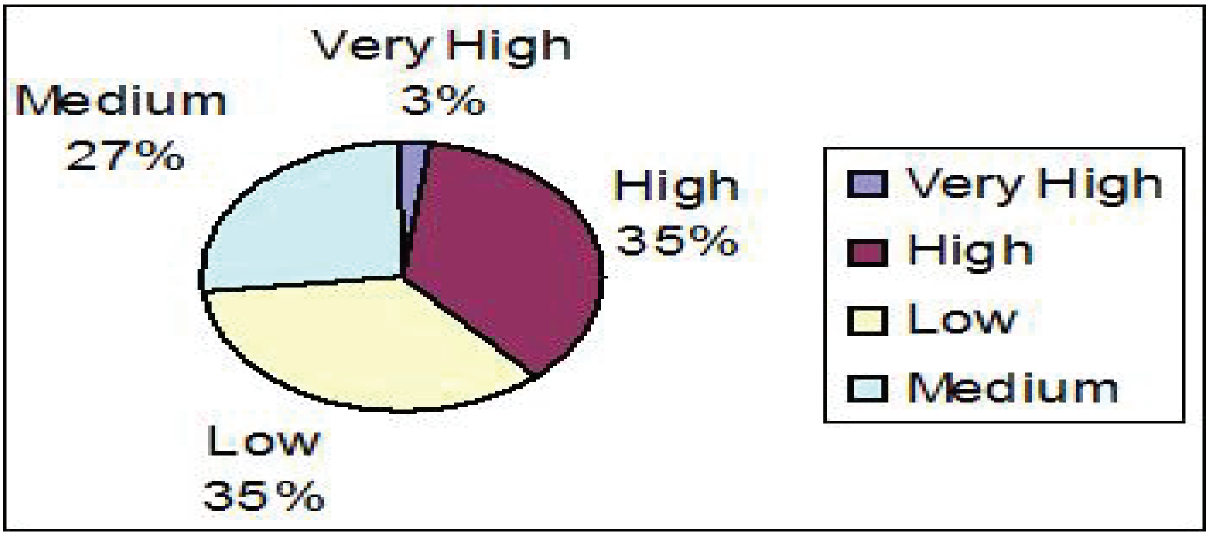

Figure 3: Risk level percentage chart

The risks which have very high values are the existence of shared administrator accounts, the lack of password policy within the active directory system and the existence of a server behind the firewall instead of the DMZ, which is accessed from the Internet.

Apart from the risks within the processes, there is another class of risk which is called general risks. General risks do not belong to a specified process; rather, they impact the whole scope and the organization itself. As another property of general risks, they may exist in more than one process. The most of the general risks are revealed as a result of ISO 27002 gap analysis. In the case study, nineteen general risks are found. Seven of them are very high and the others are high. Some of the general risks are shown in Table 11.

Table 11: Some of the general risks

General Risk	Risk Level
The lack of an information security policy document	Very High
The lack of an asset inventory	High
The lack of information security trainings	High

Up to now, the results of the risk analysis process are presented. After the risk analysis processes, these risks are evaluated, their degrees of assurance are determined, countermeasures are suggested, costs and the importance of countermeasures are listed and risks are prioritized. Finally, the countermeasures are determined.

After this process, 45 percent of the risks are eliminated by determining and applying countermeasures, these are called quick wins. 50 percent of the risks are planned to be eliminated or decreased in the specified period, which is stated in the risk treatment plan. 5 percent of the risks are accepted because of high countermeasure costs.

The application of our risk analysis method lasted about four weeks from scratch. The scope was broad enough to last four weeks. Before starting the risk analysis process, a risk analysis team was put together. There were five employees of the organization in this team. It would not be useful to run this process entirely detached from the employees. This would be an inconsistent approach for information security risk analysis. The employees worked without any ambiguity on the method and during the entire process they participated in the selection of the assets, vulnerability, threat and risk evaluations and countermeasure selection. As a result, they reached compromises on the values of assets, threats and finally risks.

Study within the organization showed that, our risk analysis method is in tune with the nature of information security risk analysis. Information security risk analysis processes should include the discussions and decisions of the involved people. As stated in the introduction, complicated mathematical and statistical tools would have limited use in modeling the risks of information security.

Another important point was to use ISRAM within the process. The results of the survey were vital input for the core risk analysis process. The ISRAM process was conducted for the employee surveys and distributed to more than one hundred employees. The systematic structure of ISRAM eased the survey preparation and evaluation processes. Performing the whole risk analysis process only by using ISRAM would not be suitable as stated in the introduction. However, ISRAM fits well into the employee survey step of our risk analysis process, since it is used as an aid.

5. Conclusion

To conclude, a systematic process should be followed to analyze risks. In the information security domain, user involvement is an important part of the process. The risk analysis method for information security should allow effective participation of the employees in the process. If the risk analysis method contains complicated mathematical and statistical tools, it will be extremely difficult to model the system. Even if the model is constructed, it will require the participation of experts and it will take a very long time.

Our proposed collaborative paper-based and qualitative risk analysis method allows company workers to perform the risk analysis. It does not contain complicated mathematical tools. It is a systematic method, so that asset valuations, threat valuations, countermeasure prioritizations are performed by using reference tables. The proposed method fulfils the requirements that are stated in the ISO/IEC

27001:2005 standard and is especially designed for companies that pursue ISO/IEC 27001:2005 certification. The results of the process exercise in the organization confirmed these statements.

It is said that, the official ISO/IEC 27001:2005 route can be very difficult because of its “all-or-nothing” design and an incremental approach to certification is suggested (Solms 2001). We think that it is possible to cover all of the sections of ISO/IEC 27002:2005 in just one step in a reasonable time period with our collaborative process based risk analysis methodology.

Another important conclusion about the proposed risk analysis method is its harmony with corporate governance. Our collaborative process based risk analysis reveals crucial business processes within its scope and analyzes the business risks for these processes. Traditionally, a great deal of attention is focused on efforts that address the risks affecting business information from an IT infrastructure point of view (Posthumus 2004). The proposed method does not put an emphasis on technical items such as servers and software, rather, it accents business processes. Thus, it complies with corporate governance principles.

References

International Organization for Standardization-ISOa (2005) “ISO/IEC 27001:2005, “Information Technology - Security Techniques - Information Security Management Systems - Requirements”

International Organization for Standardization-ISOb (2005) “ISO/IEC 27002:2005, “Information Technology - Security Techniques - Code of Practice for Information Security Management”

Computer Fraud & Security-CFS (2003) “BS7799 – Slow Uptake by Companies”, doi:10.1016/S1361-3723(03)03005-7

Karabacak, B. and Sogukpinar, I. (2006) “A Quantitative Method for ISO 17799 Gap Analysis”, *Computers & Security,* Vol. 25, Issue 6, pp. 413 – 419.

Karabacak, B. and Sogukpinar, I. (2005) “ISRAM: Information Security Risk Analysis Method”, *Computers & Security,* Vol. 24, Issue 2, pp. 147 – 159.

Aven, T. and Rettedal W. (1998) “Bayesian Frameworks for integrating QRA and SRA Methods”, *Structural Safety*, Vol. 20, pp. 155 – 165.

Ru, W. G. and Eloff, J. H. P. (1996) “Risk Analysis Modelling with the Use of Fuzzy Logic”, *Computers & Security*, Vol. 15, No.3, pp 239 – 248

Staker, R. J. (1999) “Use of Bayesian Belief Networks in the Analysis of Information System Network Risk”, *Information, Decision and Control, IDC 99 Proceedings*, pp. 145 – 150

Bilbao A. (1992) “TUAR. A model of risk analysis in the security field”, *International Carnahan Conference on Crime, Countermeasures, Proceedings. Institute of Electrical and Electronics Engineers*, pp. 65 - 71

National Institute of Standards and Technology-NIST (2001) “NIST Special Publication 800-26, Security Self Assessment Guide for Information Technology Systems”

McEvoy, N. and Whitcombe, A. (2002) “Structured Risk Analysis”, Paper read at the International Conference on Infrastructure Security, InfraSec 2002, Bristol, UK.

United States General Accounting Office-USGAO (1999) “Information Security Risk Assessment” http://www.gao.gov/cgi-bin/getrpt?GAO/AIMD-00-33.

Kim, T. and Lee, S. (2005) “Design Procedure of IT Systems Security Countermeasures”, *Computational Science and Its Applications*, Vol. 3481/2005, pp. 468 – 473

Yeh, Q. and Chang, A. J. (2007) “Threats and Countermeasures for Information System Security: A Cross-Industry Study”, *Information & Management*, Vol. 44, pp. 480 – 491

Tong, C., K., S., Fung K. H., Huang H. Y. H and Chan K. K. et al. (2003) “Implementation of ISO17799 and BS7799 in Picture Archiving and Communications System: Local Experience in Implementation of BS7799 Standard”, Paper read at CARS 2003, Computer Assisted Radiology and Surgery, proceedings of the 17th International Congress and Exhibition, London, UK.

Solms, B. and Solms, R. (2001) “Incremental Information Security Certification”, *Computers & Security*, Vol. 20, No. 4, pp. 308-310.

Posthumus, S. and Solms, R., (2004) “A framework for the governance of information security”, *Computers & Security*, Vol 23, pp. 638-646.