

QUANTITATIVE MANAGEMENT  
OF  
INFORMATION SECURITY IN ORGANIZATIONS

A THESIS SUBMITTED TO  
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES  
OF  
ÇANKAYA UNIVERSITY

BY

OĞUZHAN ŞEREFLİŞAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR  
THE DEGREE OF MASTER OF SCIENCE  
IN  
COMPUTER ENGINEERING

DECEMBER, 2016


Title of the Thesis: **Quantitive management of Information Security in organizations.**

Submitted by **Oğuzhan Şereflişan**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University

  
Prof. Dr. Halil Tanyer EYYUBOĞLU  
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

  
Prof. Dr.  
Müslim BOZYİĞİT  
Head of Department

This is to certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

  
Supervisor

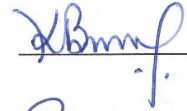
**Examination Date :**

26-12-2016

**Examining Committee Members**

Prof.Dr.Kemal BIÇAKCI

TOBB ETÜ



Assist. Prof. Dr. Reza ZARE  
HASSANPOUR

Çankaya Univ.



Assist. Prof. Dr. Abdül Kadir GÖRÜR

Çankaya Univ.



## STATEMENT OF NON-PLAGIARISM

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Oğuzhan ŞEREFLİŞAN

Signature :



Date :

26.12.2016



## ABSTRACT

### QUANTITATIVE MANAGEMENT OF INFORMATION SECURITY IN ORGANIZATIONS

Şereflişan, Oğuzhan

M.Sc., Department of Computer Engineering

**Supervisor:** Assist. Prof. Dr. Reza ZARE HASSANPOUR

December 2016, 111 pages

Different methodology implementation to define quantitative management of information security in organizations including defining information risks quantitative approach using Lenstra and Voss [1] suggestion, *annual loss expectancies* like model to meet the expectations of the real world applications like cost management, finance management etc. We made some improvements on approach using ISO/IEC 27005:2011 framework. It was chosen because of a global standard and included in ISO 31000:2009, also my real life experiences deal with ISO/IEC 27001 implementation and certification.

**Keywords:** Quantitative management, Information Security, Risk Assessment, ISO/IEC 27005.

## ÖZ

### KURULUŞLARDAKİ BİLGİ GÜVENLİĞİNİN

### ÖLÇÜLEBİLİR YÖNETİMİ

Şereflişan, Oğuzhan

Yüksek Lisans., Bilgisayar Mühendisliği Anabilim Dalı

**Tez Yöneticisi:** Y.Doç.Dr. Reza ZARE HASSANPOUR

Aralık 2016, 111 sayfa

Gerçek dünyadaki maliyet yönetimi, finans yönetimi vb. konulardaki gerçeklikleri ve beklentileri karşılayacak nitel olarak ölçülebilir bilgi risklerinin tanımlanması ve ölçülebilir yönetilen bilgi güvenliği altyapısı için Lenstra ve Voss [1] tarafından önerilen *yıllık kayıp beklentileri* ne benzeyen metodolojide, ISO/IEC 27005:2011 çerçevesi dâhilinde iyileştirme yapılarak, uygulanması işlenmektedir. Dünya çapında geçerliliği olan ve ISO 31000:2009 içine dâhil edilmiş olmasının yanında ISO/IEC 27001 uygulama ve sertifikasyon konusundaki gerçek hayat uygulamaları tecrübelerimin ağır basmasından dolayı ISO/IEC 27005 de belirlenen Risk Yönetim çerçevesi dâhilinde uygulama için seçmiş bulunmaktayız.

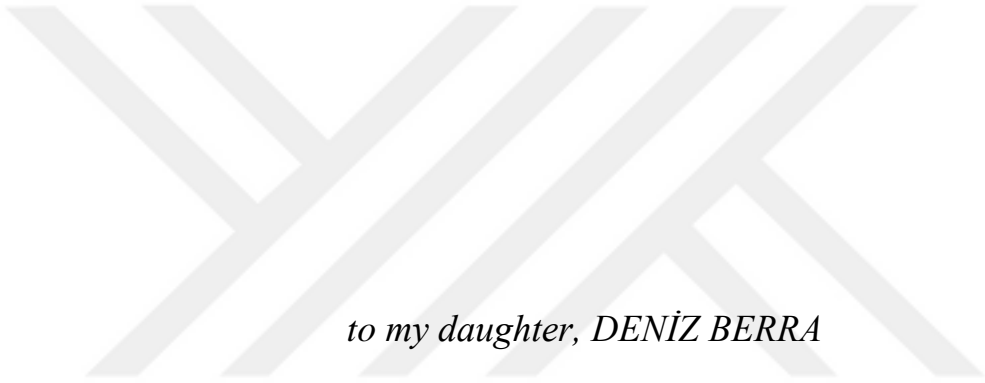
**Anahtar Kelimeler:** Nicel yönetim, Bilgi Güvenliği, Risk Değerlendirmesi, ISO/IEC 27005.

## ACKNOWLEDGMENTS

I would like to thank to my thesis advisor Assist. Prof. Dr. Reza ZARE HASSANPOUR who has guided me with his valuable ideas patiently during the preparation of this thesis. Also I would like to thank to Assist. Prof. Dr. Abdül Kadir GÖRÜR and Prof. Dr Kemal BIÇAKCI who have shared valuable ideas with me through the preparation of this thesis.

I had useful discussions with Jarno Roos I would like to thank him cordially for his valuable comments.

I wish to thank the examining committee for their kindness during the presentation of this thesis.



*to my daughter, DENIZ BERRA*

## TABLE OF CONTENTS

STATEMENT OF NON-PLAGIARISM .....	<b>Error! Bookmark not defined.</b>
ABSTRACT .....	iv
ÖZ .....	v
ACKNOWLEDGMENTS .....	vi
TABLE OF CONTENTS .....	viii
LIST OF TABLES .....	xi
LIST OF FIGURES .....	xii
LIST OF ACRONYMS .....	xiii
CHAPTER I INTRODUCTION .....	14
CHAPTER 2 THE ANNUAL LOSS EXPECTANCY-LIKE MODEL FROM LENSTRA AND VOSS .....	16
1.2 Action plans to reduce the risks .....	20
1.3 New approach .....	23
CHAPTER 3 RISK ASSESSMENT MODELS ANALYSIS AND THE EXAMINATION OF ISO/IEC 27000 SERIES .....	24
2.1 SPRINT [2] (Simplified Process for Risk Identification): .....	24
2.2 SPARK [4]: .....	24
2.3 FIRM Scorecard [5]: .....	25
2.4 SP800-30 [6]: .....	25
2.5 CORAS [7] : .....	26
2.6 OSSTMM-RAV : .....	29
2.7 ISO/IEC 27000 SERIES [8] .....	29
2.7.1 ISO/IEC 27000:2016 .....	31
2.7.2 ISO/IEC 27001:2013 .....	31



2.7.3 ISO/IEC 27002:2013 .....	32
2.7.4 ISO/IEC 27003:2010 .....	32
2.7.5 ISO/IEC 27004:2009 .....	32
2.7.6 ISO/IEC 27005:2011 .....	33
2.7.7 ISO/IEC 27006:2015 .....	33
2.7.8 ISO/IEC 27007:2011 .....	34
2.7.9 ISO/IEC 27008:2011 .....	34
2.7.10 ISO/IEC 27009:2016 .....	34
2.7.11 ISO/IEC 27010:2015 .....	35
2.7.12 ISO/IEC 27011:2016 .....	35
2.7.13 ISO/IEC 27013:2015 .....	35
2.7.14 ISO/IEC 27014:2013 .....	36
2.7.15 ISO/IEC TR 27015:2012 .....	36
2.7.16 ISO/IEC TR 27016:2014 .....	36
2.7.17 ISO/IEC 27017:2015 .....	36
2.7.18 ISO/IEC 27018:2014 .....	37
2.7.19 ISO/IEC TR 27019:2013 .....	37
2.7.20 ISO/IEC 27021:2011 .....	38
2.7.21 ISO/IEC 27023:2015 .....	38
2.7.22 ISO/IEC 27031:2011 .....	38
2.7.23 ISO/IEC 27032:2012 .....	39
2.7.24 ISO/IEC 27033 .....	39
2.7.25 ISO/IEC 27034 .....	40
2.7.26 ISO/IEC 27035:2016 .....	41
2.7.27 ISO/IEC 27036 .....	41
2.7.28 ISO/IEC 27037:2012 .....	42
2.7.29 ISO/IEC 27038:2014 .....	42
2.7.30 ISO/IEC 27039:2015 .....	43
2.7.31 ISO/IEC 27040:2015 .....	43
2.7.32 ISO/IEC 27041:2015 .....	44
2.7.33 ISO/IEC 27042:2015 .....	44
2.7.34 ISO/IEC 27043:2015 .....	45
2.7.35 ISO/IEC 27050:2016 .....	45

2.7.36 ISO 27789:2013 .....	46
2.7.37 ISO 27799:2016.....	46
2.7.38 IN DEPTH OF ISO/IEC 27005/2011 .....	47
CHAPTER 4 COMBINING OF ALE MODEL BY LENSTRA and VOSS [1]	
APPROACH AND NEW MODEL .....	55
3.1 OBJECTIVES .....	56
3.2 QUESTIONS .....	57
3.3 NEW MODEL.....	60
CHAPTER 5 REAL LIFE APPLICATIONS WITH NEW MODEL .....	68
4.1 Collected Information.....	69
4.2 Importance values definition .....	77
4.3 Current likelihood indicator calculation.....	78
4.4 Calculation of assets' financial value using new model.....	81
CHAPTER 6 CONCLUSION AND THE FUTURE WORK .....	87
REFERENCES.....	88
APPENDIX A .....	90
APPENDIX B .....	110
CURRICULUM VITAE .....	110

## LIST OF TABLES

Table A - Synonyms	xiii
Table 1.1 Loss symbols	17
Table 1.2 Type of loses	19
Table 1.3 IS Risk indicator	19
Table 2.1 OSSTMM-RAV calculation basis	29
Table 3.1 Estimated importance values	62
Table 3.2 Depreciation definitions	64
Table 4.1 Asset values of the organization	70
Table 4.2 Asset values matching table with CIA	71
Table 4.3 Possibility values of risks	71
Table 4.4 Damage values of risks to assets	71
Table 4.5 Sample asset's importance values	77
Table 4.6 Risk scores of example risk "The operating system is unable to serve" for sample asset	79

## LIST OF FIGURES

Figure 2.1 CORAS method steps	26
Figure 2.2 ISO/IEC 27005 Risk assessment process	49
Figure 2.3 ISO/IEC 27005:2008 PDCA Model	52
Figure 4.1 Physical Assets List	72
Figure 4.2 Software Assets List	73
Figure 4.3 Information Assets List	74
Figure 4.4 Human Resources Assets List	75
Figure 4.5 Services Assets List	76
Figure 4.6 Software assets' risks	78
Figure A.1 Software-menu screenshot	105
Figure A.2 Software-Inventory definition screenshot	105
Figure A.3 Software-risk definition screenshot	105
Figure A.4 Software-Control definition screenshot	106
Figure A.5 Software-Threat definition screenshot	106
Figure A.6 Software-Vulnerability definition screenshot	107
Figure A.7 Software-Risk matching	107
Figure A.8 Software-Inventory Analysis	107
Figure A.9 Software-Threat analysis screenshot	108
Figure A.10 Software-Threat analysis screenshot 2	108
Figure A.11 Software-Vulnerability analysis screenshot	108
Figure A.12 Software-MS Excel Export	109
Figure A.13 Software-MS Word Export	109

## LIST OF ACRONYMS

FTS 2001[2]	Federal Technology Service - 2001
ALE	Annual Loss Expectancies
ISP	Internet Service Provider
RAV	Risk Assessment Value
OpSec	Operational Security
ActSec	Actual Security
LC	Loss Controls
ISMS	Information Security Management System
PDCA	Plan-Do-Check-Act
COBIT	Control Objectives for Information and Related Technology
PCI-DSS	Payment Card Industry Data Security Standard
ICT	Information and Communication Technology
IS	Information Security
VaR	Value at Risk
IVEI	Internet and Interactive Services Department
CIA	Confidentiality-Integrity-Availability

Table A- Acronyms

## CHAPTER I

### INTRODUCTION

Today, the value of information has been getting more important and valuable because of dependency of organizations to the correct operation of their information have become increasing in a big situation. While business environments become more complex and variable, losses in the areas increase because of mismanagement or wrong strategy of information security management. Organizations want to use risk management frameworks to manage information security and control their risks and try to reduce their effects on the systems deal with information processing. According to the general idea, organizations tend to give this responsibility, due to name perhaps, to Information Systems Departments. This idea is a wrong way of implementation of information security management system.

Due to general experiences, implementing and managing any information risk management system is not just a matter of implementation of *good practices*. Sometimes, more risk will be present than defined acceptable level and we have to choose additional countermeasures to reduce the risk to defined acceptable level due to business nature. This brings forward the need for a method that gives control over, and a more detailed insight in the information risk of an organization. Building up an information security management system, it is known that the risks must be identified and then evaluated. Risk identification methods will be explained but the aim of this thesis focusses on a quantitative approach to calculate risk scores in contrast to a qualitative approach. Earlier generations of quantitative approaches had the drawbacks of not including financial values of assets which are affected by the threats, being excessively complex to implement real world, unable to deal with uncertainty and being highly dependent on the availability of sparse information. Nevertheless, the

currently often used qualitative approaches which are not based on real values and realities, do not give the desired results in all situations, indicating the need for a different approach.

The main aim of thesis is to propose a quantitative computational method which calculates the closest cost value of information security and the elements it contains. By adding defined any quantitative computational method to a suitable qualitative risk assessment methodology, we try to get insight in the usability of a quantitative approach in the risk scoring in information security practice. By conducting expert interviews within some specific companies working on telecommunications and production areas by doing literature review, requirements have been formulated on the applicability of a computational method and on the suitability of current risk assessment methodologies.

This thesis has the following organization:

In Chapter 2, we are going to define ALE approach of Lenstra and Voss [1].

In Chapter 3, we are going to analyze ISO/IEC 27000 series' all standards and technical guides, drafts. Also ISO/IEC 27005 Risk Management framework will be explained in detail.

In Chapter 4, we are combining ALE-like model determined by Lenstra and Voss [1] and our new model using ISO/IEC 27000 series and ISO/IEC 27005 Risk Management framework.

In Chapter 5, we apply the new model to real life risk documentation and get the results of defining the quantitative value of risks.

In Chapter 6, we are explaining how anyone can develop this model and showing a way for future work.

## CHAPTER 2

### THE ANNUAL LOSS EXPECTANCY-LIKE MODEL FROM LENSTRA AND VOSS [1]

Today's world of business creates, uses and destroys lots of information even in seconds. Also there are competitors or counter-minded people who want rival's information using legal or illegal ways. Illegal ways create some threats for vulnerabilities of the assets which are used to process the information. So the information processors are developing themselves like new software versions, new hardware using new technology. Of course new things may have unknown bugs or vulnerabilities if they are not fully tested for all scenarios of real life. The new technology sometimes so complex to manage and this may be the problem about to have new vulnerabilities. "So vulnerabilities that may threaten the security of a company's data, how does the company decide where to spend its IS budget to limit as much as possible the damaging consequences of attacks? Traditionally, this decision-making process is mostly left to *experienced* staff whose judgment, intuition, and taste is relied upon" [1].

"Each business process is exposed to a certain *current Information Security risk*. As a consequence, the organization is exposed to the total of current Information Security risks of its business processes: it is known as *current aggregated Information Security (IS) risk*. Each business process uses a number of applications, where a single application may be used by more than one process" [1] and the opposite is possible also. Each application used by business processes has some vulnerability and those can be identified. After identifying those vulnerabilities, the threats deal with those vulnerabilities can be determined also. To define the IS Risk which works in a rapidly



changing environment including threats, vulnerabilities etc. and that allows meaningful aggregation, then IS risk must be defined as a simple expected value of some sort.

Due to ISO/IEC 27001 [3], the IS risks effecting a business process are due to a breach of confidentiality, integrity, or availability. It is stated [1] that for each of these categories the user enters an estimated loss amount, denoted for business process  $p$  by  $L_c(p)$ ,  $L_i(p)$  and  $L_a(p)$  respectively. Because of any high value loss amount is so effective on assets value, the value is assumed that  $\max(L_c(p), L_i(p), L_a(p)) > 0$ .

Symbol	Explanation
$p$	Business process
$L_c(p)$	Estimated loss amount of confidentiality
$L_i(p)$	Estimated loss amount of integrity
$L_a(p)$	Estimated loss amount of availability

Table 1.1 Loss symbols

The likelihood those losses defined in the Table 1.1 are actually incurred depends on the threats uses vulnerabilities in the process (or rather: the threats realizing the vulnerabilities identified in the applications used in the process). According to model, the user defines a threat  $t$  by selecting three *types of threat* specifications. The assumption under this calculation is defining a scale with analysts and experienced stuff and evaluation of the loss using this scale.

- “**Source of threat**, with two possible choices indicating, if the threat comes from a party *external* (Source ( $t$ ) = 1) or *internal* (Source ( $t$ ) = 0,8 ) to the company” [1].
- “**Access required for the threat**, with two possible choices indicating if remote access (Access ( $t$ ) = 1) suffices to realize the threat or if local access (Access ( $t$ ) = 0.6) is required” [1].
- “**Skill level required for the threat**, with four possible choices indicating the least level of skill required to realize the threat:

- unstructured nontechnical ( $\text{Skill}(t) = 1$ );
- unstructured technical ( $\text{Skill}(t) = 0.9$ );
- structured nontechnical ( $\text{Skill}(t) = 0.75$ );
- structured technical ( $\text{Skill}(t) = 0.25$ ).” [1]

A hacker, for instance, would be *unstructured technical*, but a script kiddie would be “unstructured nontechnical”.

Those valuations are calculated within the Lenstra and Voss [1] model and we will use those scores in our model also.

The *current likelihood indicator*  $P(t)$  of threat  $t$  is defined as

$$P(t) = \text{Source}(t) * \text{Access}(t) * \text{Skill}(t) [1]$$

“These four numeric values remain hidden for the user. A qualitative ranking of  $P(t)$ , however, is presented to the user: High if  $P(t) \geq 0.6$ , Low if  $P(t) < 0.2$ , and Medium otherwise. The user wants to change the qualitative ranking; if done so the hidden likelihood indicator is changed:

- if the user wants to specify High and  $P(t) < 0.6$ , then replace  $P(t)$  by 0.6;
- if the user specifies Medium and  $P(t) \geq 0.6$ , then replace  $P(t)$  by 0.6
- if the user specifies Medium and  $P(t) < 0.2$ , then replace  $P(t)$  by 0.2;
- if the user specifies Low and  $P(t) \geq 0.2$ , then replace  $P(t)$  by 0.2.

To indicate what type of loss can be inflicted by a threat, the user enters three bits  $T_c, T_i, T_a \in \{0, 1\}$ , where  $T_c = 1$  if and only if the threat may cause a breach in confidentiality (similar for  $T_i$  and  $T_a$  with respect to integrity and availability, respectively).” [1]

Symbol	Explanation
$T_c$	Type of loss about confidentiality
$T_i$	Type of loss about integrity
$T_a$	Type of loss about availability

Table 1.2 Type of loses

Note that these bits depend just on the threat and not on the process they may affect.

“Data about threats (as above) and action plans (as below) should be agreed upon by all businesses using that application. One business unit may originally have entered threat data and action plans for an application, but other business units affected by the same threat may review the data provided and propose changes. It is the responsibility of all parties involved to come to an agreement on the proper values. A welcome side-result of this interaction is corporate-wide consistency of (and agreement on) the *quantification* of the threats and action plans” [1].

Given these values entered by the user, the *current IS risk indicator of process p with respect to threat t* is defined as

$$R_{cur}(p, t) = \max(T_c L_c(p), T_i L_i(p), T_a L_a(p)) P(t)$$

$R_{cur}(p, t)$	The current Information Security risk indicator of process $p$ with threat $t$
-----------------	--

Table 1.3 IS Risk indicator

Denoting by  $S(p)$  the set of applications used in process  $p$  and by  $\mathcal{T}(A)$  the set of threats affecting application  $A$ , the *current IS risk indicator of process p* is defined as

$$R_{cur}(p) = \sum_{A \in S(p)} \sum_{t \in \mathcal{T}(A)} R_{cur}(p, t)$$

If  $P$  is the set of all business processes, the corporation's overall (quantitative) *current aggregated IS risk indicator* is defined as

$$R_{cur} = \sum_{p \in P} R_{cur}(p)$$

## 1.2 Action plans to reduce the risks

“For an action plan  $\alpha$  countering a threat  $t$ , denote by  $t_\alpha$  the residual threat, i.e., what remains of  $t$  after action plan  $\alpha$  has been carried out. For each action plan  $\alpha$  countering a threat  $t$  the user characterizes the residual threat  $t_\alpha$  by entering the three type of threat values  $Source(t_\alpha)$ ,  $Access(t_\alpha)$ , and  $Skill(t_\alpha)$ , similar to  $Source(t)$ ,  $Access(t)$ , and  $Skill(t)$  above except that they now represent the values after action plan  $\alpha$  has been carried out. This results in the *residual likelihood indicator*” [1]

$$P(t_\alpha) = Source(t_\alpha) * Access(t_\alpha) * Skill(t_\alpha) [1]$$

“Obviously, for an action plan to be any good, it should be the case that  $P(t_\alpha) < P(t)$ ; it is assumed that this condition holds for all threats  $t$  and action plans  $\alpha$  under consideration. As above, and using the same calculations, the qualitative ranking of  $P(t_\alpha)$  is presented to the user, who has the option to change it, which may change the value  $P(t_\alpha)$ . If the resulting  $P(t_\alpha)$  happens to be larger than  $P(t)$ , which may happen if the user manually changed  $P(t)$  or  $P(t_\alpha)$  values,  $P(t_\alpha)$  is set to  $P(t)$ ; action plans for which this happens do not have to be further considered. Also this calculation may be occurring by a wrong action plan which makes threat  $t$  *risk indicator* higher than original. The user also enters the projected expense  $w(\alpha)$  of action plan  $\alpha$ . The type of loss bits are, in the present model, not affected by the action plans. Therefore, the *residual IS risk indicator of process  $p$  with respect to threat  $t$  after action plan  $\alpha$  is carried out* is defined as” [1]

$$R_{cur}(p, t_\alpha) = \max(T_c L_c(p), T_i L_i(p), T_a L_a(p)) P(t_\alpha)$$

“We assume that a single action plan can be carried out per threat or not, that action plans cannot be carried out partially, and different threats may have different action plans. This is not a restriction as seen. In situations where it makes sense to consider a fractional combination of one or more action plans countering a single threat, one simply enters the relevant fractional combination of action plans with their partial or cumulative effects (and expenses) as an alternative action plan.

There would be at most one action plan per threat in an *allowed set of action plans*.

Let  $A$  be an allowed set of action plans and let  $w(A) = \sum_{\alpha \in A} w(\alpha)$

$w(\alpha)$  be the projected expense of  $\alpha$ . *The residual IS risk indicator of process  $p$  with respect to threat  $t$  after the action plans in  $A$  are carried out is defined as” [1]*

$$R_{res}(p, t, A) = \begin{cases} R_{cur}(p, t) & \text{if } A \text{ does not contain an action plan countering threat } t \\ R_{res}(p, t_{\alpha}) & \text{if } A \text{ contains action plan } \alpha \text{ countering threat } t \end{cases}$$

and the *residual IS risk indicator of process  $p$  under allowed action plan set  $A$*  is defined as

$$R_{res}(p, A) = \sum_{A \in S(p)} \sum_{t \in \mathcal{T}(A)} R_{cur}(p, t, A)$$

Finally, the corporation’s (quantitative) *residual aggregated IS risk indicator after allowed action plan set  $A$*  is defined as

$$R_{res}(A) = \sum_{p \in P} R_{res}(p, A)$$

“Optimal risk mitigation consists of finding an allowed action plan set  $A$  that minimizes  $R_{res}(A)$ . This is trivially solved by determining for each threat  $t$  the action plan  $\alpha$  that minimizes  $P(t_{\alpha})$  (in case of conflict, select one), and by defining  $A$  as the set of those action plans (which will be allowed due to the construction). The interesting problem is the method to find an allowed action plan set  $A$  which minimizes  $R_{res}(A)$  under a budgetary constraint  $w(A) \leq W$  on  $A$ ’s projected expense.” [1]

“The current and residual aggregated IS risk indicators  $R_{cur}(p)$  and  $R_{res}(p, A)$  for a process  $p$  and allowed action plan set  $A$  must not and cannot be interpreted as the

expected loss amount for  $p$  before and after  $A$ . Any interpretation of that sort would at the very least require introduction of a temporal dependency in the model. This may be done, if required, at a later stage. Similarly, a threat's likelihood indicator  $P(t)$  should not immediately be interpreted as the probability that the threat is realized. It requires more threat related data and fine-tuning of the above parameter choices before the likelihood of a threat's occurrence can reliably be estimated based on the type of threat values. It may also be the case that for a reasonably accurate estimate more threat characteristics are required. However, we are not convinced that the disadvantage of the introduction of any extra complications (a steeper learning curve) would be outweighed by the potential advantages. At present the  $P(t)$ ,  $P(t_\alpha)$ ,  $R_{cur}(p, t)$ ,  $R_{cur}(p)$ ,  $R_{res}(p, t_\alpha)$ ,  $R_{res}(p, A)$  and  $R_{res}(p, t, A)$  values by themselves are simply not intended to be meaningful. What is relevant is the consistency that is achieved by this approach and the fact that the relative values are meaningful. That allows us to interpret terms such as  $R_{cur}(p, t)$  as expected values (of some value, up to an unknown and irrelevant constant scaling factor) and thereby to aggregate them into a quantitative IS risk indicator using simple summation, as in the definitions of  $R_{cur}(p)$ ,  $R_{cur}$ ,  $R_{res}(p, A)$  and  $R_{res}(A)$ . It also allows us to find an optimal allowed set of action plans under a budgetary constraint, as described in the next section. Note that also the values  $R_{cur}$  and  $R_{res}(A)$  by themselves are hardly meaningful. What is meaningful is the quantity

$$\frac{100 (R_{cur} - R_{res}(A))}{R_{cur}}$$

because it gives the percentage how much *better* the situation is after carrying out the action plans in  $A$ , with 0% indicating no improvement and 100% that there is no residual aggregated IS risk left (since  $R_{res}(A)=0$ ).

It may be tempting to include a weighting mechanism in the IS risks to account for *relative importance* of the various business processes. However, this may be done only if the weights are not correlated to the loss indicator values, because a correlation would undermine the soundness of the aggregation method. If risk is no longer defined as the expected value of a linear function of a loss indicator (as would

be the case if loss indicator correlated weights are included), risk aggregation can no longer be done by summation. Correct aggregation would require the distribution functions underlying the threats and their correlation behavior, leading to numerous complications and pitfalls and, if those can be solved and avoided, respectively, to considerably more involved definitions of  $R_{cur}(p)$ ,  $R_{res}(p, A)$ ,  $R_{cur}$ , and  $R_{res}(A)$ . Weights that reflect the relative importance of businesses may be used if they are independent of the amount of loss the businesses may incur due to IS failures. Obviously, this is only meaningful if the same set of weights is used in  $R_{cur}$  and  $R_{res}(A)$ . Now current model does not use weights. Using weights would be one way to include a temporal dependency in the model.” [1]

This approach does not require actual event distributions or consider complex interactions. It is based on the aggregation of expected losses done by simple summation. This simplicity makes it a flexible approach that can be easily adjusted to fit a practitioner’s requirements.

### **1.3 New approach**

We modified the annual loss expectancy model from Lenstra and Voss [1] by incorporating separate threat and vulnerability components using ISO/IEC 27005 framework, risk assessment methodology. A working example is given in Chapter 4. New model includes financial information about losses of asset used in processing information to help managers to decide about prioritization of risk mitigations and prepare plans. Of course those risk mitigation plans must be prepared under budget limits. Every company has the problem of financial limits. Because information security and risk management includes unlimited domains but sources are limited as the principal. So that the risk mitigation and prioritization issues are so important and also defining the right risks with the objective model is the right way for the continuity if risk planning. Using only the model defined by experienced stuff may be depending on subjective ideas.

## CHAPTER 3

### RISK ASSESSMENT MODELS ANALYSIS AND THE EXAMINATION OF ISO/IEC 27000 SERIES

Due to ease of defining information security risks and also defining inputs to ALE model, ISO/IEC 27005 framework is used to define risks. We would like to see when ISO/IEC 27005 framework applied to define risks and scoring them, information security risks are quantified in an objective way or not. Our new model will be explained in detail in Chapter 3 at 54. Our model looks similar to the SPARK methodology which enhanced and combined with ISO/IEC 27001-2013. But in our model of course some modifications with the models used before like SPARK, [4].

When searching about quantitative methods of risk assessment values, there are some methods like ISO/IEC 27000 series, FIRM Scorecard, SPRINT, SPARK, SP800-30, CORAS and OSSTMM-RAV. Here are the superficial analyses of those risk assessment methodologies.

#### **2.1 SPRINT** [2] (Simplified Process for Risk Identification):

“Sprint is committed to a continuing program of transition risk assessment throughout the FTS2001 contract. Sprint is also committed to providing its full cooperation to all other GSA and agency contractors to ensure that all FTS2001 transition, migration and implementation activities occur in a timely manner while minimizing impacts on the agency user communities. Risk levels are defined as *Low, Medium and High.*” [2]

#### **2.2 SPARK** [4]:

This methodology is based on the SPRINT risk analysis methodology developed by the Information Security Forum in Europe. SPARK is further enhanced and combined with ISO/IEC 27001-2013 and the more recent ISO/IEC 17799-2005 standards. Other standards (e.g. CobiT) may also be incorporated into SPARK making it very flexible.



SPARK also defines additional linkages between vulnerabilities, threats and controls are defined as compared to the SPRINT methodology. Decisions in the SPARK methodology are taken by the organization's management supported by (technical) specialists. This facilitates open communication between involved parties and leads to better alignment of IT and strategy.

### **2.3 FIRM Scorecard [5]:**

“This offer a classification system for the risks to the key dependencies in the organization. The classification system also reflects the idea that *every organization should be concerned about its finances, infrastructure, reputation and commercial success*. In order to give a broader scope to commercial success, the headings of the FIRM risk scorecard are as follows:

- F Financial;
- I Infrastructure;
- R Reputational;
- M Marketplace.

Financial and infrastructure risks are considered to be internal to the organization, while reputational and marketplace risks are external to the organization. Also, financial and marketplace risks can be easily in quantitative description. “ [5]

### **2.4 SP800-30 [6]:**

“The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process-providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. It carries out each of the steps in the risk assessment process (i.e., preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment) and how risk assessments and other organizational risk management processes complement and inform each other. Special Publication 800-30 also provides guidance to organizations on identifying specific risk factors to monitor on an ongoing basis, so that organizations can determine whether risks have increased to

unacceptable levels (i.e., exceeding organizational risk tolerance) and different courses of action should be taken.

Risk assessment is a key component of a holistic, organization-wide risk management process as defined in NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Risk management processes include: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk.” [6]

## 2.5 CORAS [7] :

“CORAS is a method for conducting security risk analysis. CORAS provides a customized language for threat and risk modeling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis. In the CORAS method a security risk analysis is conducted in eight steps:

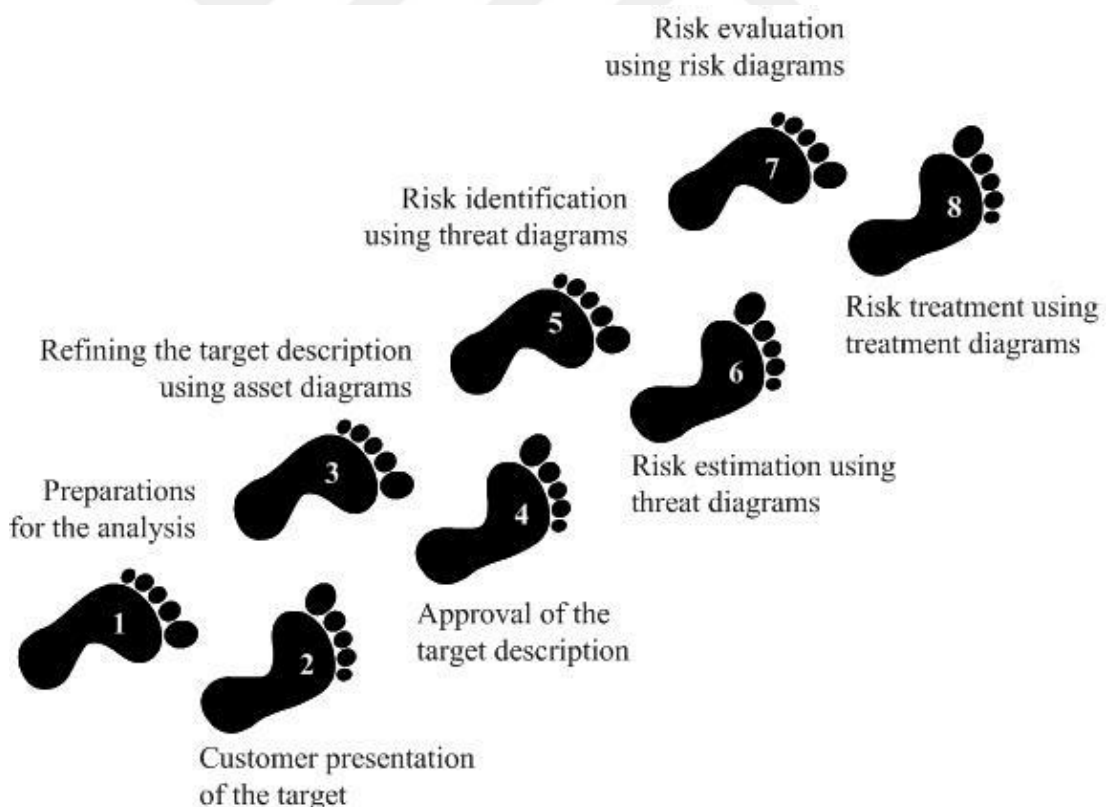


Figure 2.1 CORAS method steps

The eight steps of the CORAS method are summarized as follows.

- Step 1: The first step is the initial preparations for a risk analysis. The main objective is to get a basic idea about what is to be the target and what will be the size of the analysis such that we can make the necessary preparations for the actual analysis tasks.
- Step 2: The second step is the introductory meeting with the customer on the behalf of which the analysis is conducted. The main item on the agenda for this meeting is to get the representatives of the customer to present their overall goals of the analysis and the target they wish to have analyzed. The objective is to achieve a common initial understanding of the target of analysis, and of what the parties of the analysis are most concerned about. The overall goals of the analysis are put forward, the focus and scope of the analysis are set, and the rest of the analysis is planned.
- Step 3: The third step aims to ensure a common understanding of the target of analysis, including its focus, scope and main assets. The analysis team presents their understanding of what they learned at the first meeting and from studying documentation that has been made available to them by the customer. Based on interaction with the customer, the analysis team will also identify the main assets to be protected. The analysis team furthermore conducts a rough, high-level analysis to identify major threat scenarios, vulnerabilities and enterprise level risks that should be investigated further. The outcome of Step 3 is a refined and more detailed understanding of the target description and the objectives of the analysis, which at this point are documented by the analysts.
- Step 4: The fourth step aims to ensure that the background documentation for the rest of the analysis, including the target, focus and scope is correct and complete as seen by the customer. The step involves presenting a more refined description of the target to be analyzed, including assumptions and preconditions being made. Typically, the analysts describe the target using a formal or semi-formal notation such as the UML. Before the actual risk analysis starts at the next step of the analysis process, the description of the target should be approved by the customer. Step 4 furthermore includes deciding the risk evaluation criteria for each asset. This analysis step concludes the context establishment.

- Step 5: The fifth step is the risk identification. To identify risks, CORAS makes use of structured brainstorming. Structured brainstorming is a step-by-step walkthrough of the target of analysis and is carried out as a workshop led by the analysts. The main idea of structured brainstorming is that since the workshop participants represent different competences, backgrounds and interests, they will view the target from different perspectives and consequently identify more, and possibly other, risks than individuals or a more homogeneous group would have managed. The risk identification involves a systematic identification of threats, unwanted incidents, threat scenarios and vulnerabilities with respect to the identified assets. The activities are supported by the CORAS language, and the results are documented on-the-fly by means of CORAS threat diagrams.
- Step 6: The sixth step aims to determine the risk level of the risks that are represented by the identified unwanted incidents. The unwanted incidents were documented in threat diagrams during Step 5, and these diagrams serve as the basis for the risk estimation. Step 6 is conducted as a brainstorming involving personnel with various backgrounds, and basically involves the estimation of the likelihoods and consequences of the unwanted incidents. These values in combination yield the risk level for each of the identified risks. The CORAS threat diagrams facilitate the likelihood estimation by supporting the estimation of the likelihood for threats and threat scenarios to cause the unwanted incidents.
- Step 7: The seventh step aims to decide which of the identified risks are acceptable, and which of the risks must be further evaluated for possible treatment. Whether or not the risks are acceptable is determined by using the already defined risk evaluation criteria and the results of the risk estimation. Step 7 furthermore involves estimating and evaluating risks with respect to indirect assets.
- Step 8: The eighth step is concerned with the identification and analysis of treatments. The risks that are found to be unacceptable are evaluated to find means to reduce them. A treatment should contribute to reduced likelihood and/or consequence of an unwanted incident. Since treatments can be costly, they are assessed with respect to their cost-benefit, before a final treatment plan is made.” [7]

## 2.6 OSSTMM-RAV:

Risk Assessment Value (RAV) needs 3 values for calculation. Those are your Operational Security (OpSec), your Actual Security (ActSec) and the number of Loss Controls (LC) that you have in place. In order to begin, you must first associate all of your input information into the appropriate categories:

Operational Security	1	Visibilities
	2	Trusts
	3	Accesses
Actual Security	1	Vulnerabilities
	2	Weaknesses
	3	Concerns
	4	Exposures
	5	Anomalies
Loss Controls	1	Authentication
	2	Repudiation
	3	Confidentiality
	4	Privacy
	5	Indemnification
	6	Integrity
	7	Safety
	8	Usability
	9	Continuity
	10	Alarm

Table 2.1 OSSTMM-RAV calculation basis

## 2.7 ISO/IEC 27000 SERIES [8]

The ISO/IEC 27000-series help all type of organizations to implement and operate an Information Security Management System (ISMS). It is a popular choice. This is mostly because of the international recognition ISO standards receive worldwide.

The series provide best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series). The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks and then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities that tries to find to address changes in the threats, vulnerabilities or impacts of information security incidents.

“The series also introduce Deming's Plan-Do-Check-Act (PDCA) model which is fundamental to this series. The PDCA model works as follows:

(Plan) The process that an organization lists all its information security requirements as well as why it needs information security.

(Do) Implement and execute the controls to manage information security risks.

(Check) The effectiveness and performance of controls is checked.

(Act) Continuous improvement based on objective measurements.

An ISMS helps protect information assets based upon risk assessments and the organization's risk acceptance. The design and operation of the ISMS reflects the information security requirements of all of the organization's stakeholders. An ISMS is not only a set of technical solutions but it also includes management controls and procedures for the organization. The implementation of an ISMS starts with identifying the information assets and their security requirements. Then the information security risks are assessed and risk controls implemented. To keep the ISMS effective, the organization needs to monitor, maintain and improve controls. After an ISMS implementation the risks could change that require different or new controls.” [8]

Several factors effects a successful implementation of an ISMS such as; information security requirements of the company ; continually monitor and improve satisfying the

requirements; risk management; management commitment; employee awareness and training; business continuity management; incident response; and measurements for performance and improvement. ISMS helps organizations about lowering information security risks; supporting corporate risk management; educating and training; implementing good information security practices with adaptation to the organizations needs; possibility to get certification of the ISO/IEC 27001.

The ISO/IEC 27000 Series include the following standards [8]:

### **2.7.1 “ISO/IEC 27000:2016 Information security management systems - Overview and vocabulary” [9]**

“The ISO/IEC 27000:2016 is entitled ‘Information security management systems - *Overview and vocabulary*’. It provides an overview of and an introduction to the ISO/IEC 27000-series. It also provides a vocabulary of fundamental terms and definitions used throughout the rest of the ISO/IEC 27000-series and the relations between the standards. The standard also defines the concept of an ISMS and provides a description of the PDCA cycle. It is available as a free download.” [9]

### **2.7.2 “ISO/IEC 27001:2013 Information security management systems – Requirements” [9]**

“The ISO/IEC 27001:2013 is entitled “Information security management systems – *Requirements*”. This standard formalizes the normative requirements for development and operation for an ISMS for all types of organizations. The standard also introduces controls (in Annex A) for controlling and mitigating risks. Because of the normative nature of the ISO/IEC 27001 standard, organizations can audit and certify their ISMS by an accredited certification authority. There is a direct relationship between the controls in “Annex A” and the controls in ISO/IEC 27002.” [9]

### **2.7.3 “ISO/IEC 27002:2013 Code of practice for information security management” [9]**

“The ISO/IEC 27002:2013 is entitled “Code of practice for information security controls”. The ISO/IEC 27002 is a revised and improved version of the ISO/IEC 17799 standard. The ISO/IEC 27002:2013 standard provides more information on the controls from ISO/IEC 27001 Annex A. The standard starts with 5 introductory chapters and followed by 14 main chapters. It guides organizations in selecting and implementing information security controls. It is not possible for organizations to certify compliance against ISO/IEC 27002. Certification is done based on ISO/IEC 27001.” [9]

### **2.7.4 “ISO/IEC 27003:2010 Information security management system implementation guidance” [9]**

“The ISO/IEC 27003 provides implementation guidance to help those implementing the ISO27k standards. It describes the process of ISMS specification and design from inception to the production of implementation project plans, covering the preparation and planning activities prior to the actual implementation, and taking in key elements.” [9]

### **2.7.5 “ISO/IEC 27004:2009 Information security management – Measurement” [9]**

“The ISO/IEC 27004 concerns measurements relating to information security management: these are commonly known as ‘security metrics’ in the profession. The standard is intended to help organizations measure, report on and hence systematically improve the effectiveness of their Information Security Management Systems. It “provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.” [9]



### **2.7.6 “ISO/IEC 27005:2011 Information security risk management” [9]**

“The ISO/IEC 27005:2011 is entitled “Information security risk management”. The standard helps the organization like providing guidelines for process oriented information security risk management. It is not a specific methodology on risk management. The standard begins with a context establishment, which is the first criteria needed for risk management. The context also comprises the primary processes and supporting assets, called scope, boundaries. The next step is the risk assessment. In this step of the analysis, To identify and estimate of risks, establishing the risk management context is needed. The first step of risk identification is the identification of assets together with the vulnerabilities and threats. The second step should be finding existing controls for those threats. The next step is quantitatively or qualitatively assess the vulnerabilities and threats that exploit them. It would be useful to identify the consequences of a successful exploit. Now there is enough information to estimate the risks. This can be done by qualitative or by quantitative estimations. In addition, the organization needs to assess the risk consequences and likelihood.

The standard defines risk treatment as the next step which is not included in that thesis. As described in other parts of the ISO/IEC27000 series, an organization can choose four alternatives to deal with a risk. Those are; implementing controls; accepting the risk; avoid the risk; transfer the risk. This title will explained in detail at 2.7.38 section on *page 47*.

### **2.7.7 “ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems” [9]**

ISO/IEC 27006:2015 is entitled Information technology - *Security techniques - Requirements for bodies providing audit and certification of information security management systems*. The organizations which certify other organizations compliance with ISO/IEC 27001 uses ISO/IEC 27006 as a guide. Any accredited body providing ISO/IEC 27001 compliance certificates must fulfill those in ISO/IEC 27006, ISO/IEC 17021-1 and ISO 19011.

### **2.7.8 “ISO/IEC 27007:2011 Guidelines for information security management systems auditing” [9]**

ISO/IEC 27007:2011’s current title is Information technology - *Security techniques -- Guidelines* for Information security management systems auditing. For those auditing ISMSs for various purposes other than certified compliance with ISO/IEC 27001 use ISO/IEC 27007 as a guide (which is covered by ISO/IEC 27006). Those auditing purposes such as:

- Managing the ISMS audit programme;
- Performing an ISMS audit;
- Managing ISMS auditors.

### **2.7.9 ISO/IEC 27008:2011 Guidelines for auditors on information security controls [3]**

The technical complementary of ISO/IEC 27007 is provided by these guidelines. It’s focus is on auditing the information security controls. This is a guide for all auditors regarding *information security management systems controls* selected through a risk-based approach. It supports the information security risk management process and internal, external and third-party audits of an ISMS by explaining the relationship between the ISMS. It provides guidance on how to verify the extent to which required “ISMS controls” are implemented.

There is another workaround labelled like “ISO/IEC 27008 Guidelines for the assessment of information security controls” but it is under development.

### **2.7.10 “ISO/IEC 27009:2016 Sector-specific application of ISO/IEC 27001 – Requirements” [9]**

“ISO/IEC 27009:2016 defines the requirements for the use of ISO/IEC 27001 in any specific sector (field, application area or market sector). It explains how to include requirements additional to those in ISO/IEC 27001, how to refine any of the ISO/IEC 27001 requirements, and how to include controls or control sets in addition to ISO/IEC

27001:2013, Annex A. It ensures that additional or refined requirements are not in conflict with the requirements in ISO/IEC 27001.” [19]

#### **2.7.11 “ISO/IEC 27010:2015 Information security management for inter-sector and inter-organizational communications” [9]**

This is a guide for sharing information on information security risks, controls, issues and/or incidents that draw the boundaries between industry sectors and/or nations, particularly those affecting *critical infrastructure*.

#### **2.7.12 “ISO/IEC 27011:2016 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002” [9]**

“This implementation guide is for the telecoms industry. It was developed by ITU-T and ISO/IEC JTC1/SC27.

#### **2.7.13 “ISO/IEC 27013:2015 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1” [9]**

This standard provides guidance for implementing both ISO/IEC 27001 (ISMS) and ISO/IEC 20000-1:2011 together. Two management systems that complement and support each other’s aims.

The standard tells about a framework for organizing and prioritizing activities, offering advice on:

- Aligning the information security and service management and improvement objectives;
- Coordinating multidisciplinary activities;
- A collaborative system of supporting documents and processes (policies, working guides etc.);
- A shared vision and common vocabulary;
- Combined business benefits to customers and service providers; and
- Combined auditing of both management systems at the same time.

#### **2.7.14 ISO/IEC 27014:2013 Governance of information security [3]**

This standard is a guide for concepts and principles for the governance of information security and is applicable to all types and sizes of organizations.

The proper governance of information security process ensures *alignment* for information security with business strategies and objectives. It supports the achievement of *visibility, agility, efficiency, effectiveness* and *compliance*.

#### **2.7.15 ISO/IEC TR 27015:2012 Information security management guidelines for financial services [3]**

This guideline is a sector-specific guideline and it helps the financial services organizations (banks, credit card companies etc.) to implement ISMS using the ISO/IEC 27000 standards.

The ISMS implementation guidance developed by SC27 reflects ISO/IEC 27001 and 27002 along with various general-purpose security standards such as COBIT and the PCI-DSS requirements.

#### **2.7.16 “ISO/IEC TR 27016:2014 Information security management - Organizational economics” [9]**

“ISO/IEC TR 27016:2014 provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources.” [9]

#### **2.7.17 ISO/IEC 27017:2015 Code of practice for information security controls based on ISO/IEC 27002 for cloud services [9]**

“This standard guides cloud computing companies or services for information security and recommends and assists for cloud-specific information in coordination with ISO/IEC 27002 and other ISO27k standards. The guide additional information security

controls implementation advice other than provided in ISO/IEC 27002, in the cloud computing systems.” [3]

#### **2.7.18 “ISO/IEC 27018:2014 Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors” [9]**

“This standard provides guidance aimed at ensuring that cloud service providers (such as Amazon and Google) offer suitable information security controls to protect the privacy of their customers’ clients by securing PII (Personally Identifiable Information) entrusted to them.

The standard will be followed by ISO/IEC 27017 covering the wider information security angles of cloud computing, other than privacy.

The project had widespread support from national standards bodies plus the Cloud Security Alliance.” [3]

#### **2.7.19 ISO/IEC TR 27019:2013 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry [9]**

ISO/IEC TR 27019:2013 can be used to implement information security controls for process control systems as used in the energy utility industry. This allows the energy utility industry to implement a standardized information security management system (ISMS) in accordance with ISO/IEC 27001.

This includes in particular the following systems, applications and components:

- the IT-supported central and as well as IT systems used for their operation, such as programming and parameterization devices for process control, monitoring and automation technology;
- digital controllers and automation components;
- all further supporting IT systems used for process control;
- the communications technology used in for process control;
- digital measurement and metering devices;
- digital safety and protection systems;

- distributed components of future smart grid environments;
- all software, firmware and applications installed on above mentioned systems.

the conventional or classic control equipment that is non-digital is outside the scope of ISO/IEC TR 27019:2013. Energy process control systems in private households and other, residential building installations are outside the scope of ISO/IEC TR 27019:2013.

There is another workaround labelled like “*ISO/IEC 27019 Information security controls for the energy utility industry*” but it is under development.

### **2.7.20 “ISO/IEC 27021:2011 Competence requirements for information security management system professionals (Draft)” [9]**

“In order to stabilize the market for training and certifying professionals for ISO27k implementation and audits, a standard is planned that will lay out the competence requirements for ISMS professionals. This standard is still in draft and under development.” [3]

### **2.7.21 ISO/IEC 27023:2015 Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002 [9]**

“This is prepared as a committee document for internal use by the members of ISO/IEC JTC 1/SC 27, it was decided to publish this freely as a Technical Report and this is to show the corresponding relationship between the ISO/IEC 27001 and ISO/IEC 27002.” [3]

### **2.7.22 “ISO/IEC 27031:2011 Guidelines for information and communications technology readiness for business continuity” [9]**

“ISO/IEC 27031 guides for the concepts and principles behind the information and communications technology in ensuring business continuity.” [3]

The standard:

- Suggests a structure or framework for any organization.
- Identifies and specifies all relevant aspects for improving ICT readiness as part of the organization’s ISMS.

- Helps an organization to build up the necessary infrastructure to measure its continuity, security and readiness to survive a disaster in a consistent and recognized manner.

The scope of this standard encompasses all events and incidents (not just information security related) that could have an impact on ICT infrastructure and systems.

### **2.7.23 “ISO/IEC 27032:2012 Guidelines for cyber security” [9]**

“ISO/IEC 27032:2012 guides to improve the state of Cybersecurity. It draws out the unique aspects of that activity and dependencies on other security domains, in particular:

- information security,
- network security,
- internet security, and
- critical information infrastructure protection (CIIP).” [3]

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

- an overview of Cybersecurity,
- an explanation of the relationship between Cybersecurity and other types of security,
- defines the stakeholders and a description of their roles in Cybersecurity,
- guides to address common Cybersecurity issues, and
- a framework for collaboration between stakeholders to work together on resolving Cybersecurity issues.

### **2.7.24 “ISO/IEC 27033 Network security” [9]**

This is a multi-part standard derived from the network security standard ISO/IEC 18028. It provides detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002. It applies to the security of networked devices

and the management of their security, network applications/services and users of the network, in addition to security of information being transferred through communications links. It is aimed at network security architects, designers, managers and officers. Here are the parts:

- “ISO/IEC 27033-1:2015: network security overview and concepts” [9]
- “ISO/IEC 27033-2:2012 Guidelines for the design and implementation of network security” [9]
- “ISO/IEC 27033-3:2010 Reference networking scenarios -- threats, design techniques and control issues” [9]
- “ISO/IEC 27033-4:2014: Securing communications between networks using security gateways” [9]
- “ISO/IEC 27033-5:2013: Securing communications across networks using Virtual Private Networks (VPNs)” [9]
- “ISO/IEC 27033-6:2016: Securing wireless IP network access” [9]

#### **2.7.25 “ISO/IEC 27034 Application security” [9]**

This is a multi-part standard and it guides how to implement information security to those specifying, designing/programming or procuring, implementing and using application systems. The desired/necessary level of security is the aim for organization’s Information Security Management System. Here are the parts:

- “ISO/IEC 27034-1:2011 - Information technology - Security techniques - Application security - Overview and concepts” [9]
- “ISO/IEC 27034-2:2015 - Organization normative framework” [9]
- “ISO/IEC 27034-3 - Application security management process (Draft)” [9]
- “ISO/IEC 27034-5 - Protocols and application security controls data structure (Draft)” [9]
- “ISO/IEC 27034-6:2016 - Case studies (Draft)” [9]
- “ISO/IEC 27034-7:2016 Application security assurance prediction model (Draft)” [9]
- “ISO/IEC 27034-5-1 Protocols and application security controls data structure - XML schemas (Draft)” [9]



### **2.7.26 “ISO/IEC 27035:2016 Information security incident management” [9]**

“Information security controls are imperfect in various ways: controls can be overwhelmed or undermined (e.g. by competent hackers, fraudsters or malware), fail in service (e.g. authentication failures), work partially or poorly (e.g. slow anomaly detection), or be more or less completely missing (e.g. not [yet] fully implemented, not [yet] fully operational, or never even conceived due to failures upstream in risk identification and analysis). Consequently, information security incidents are bound to occur to some extent, even in organizations that take their information security extremely seriously.

Managing incidents effectively involves detective and corrective controls designed to recognize and respond to events and incidents, minimize adverse impacts, gather forensic evidence (where applicable) and in due course ‘learn the lessons’ in terms of prompting improvements to the ISMS, typically by improving the preventive controls or other risk treatments.

Information security incidents commonly involve the exploitation of previously unrecognized and/or uncontrolled vulnerabilities, hence vulnerability management (e.g. applying relevant security patches to IT systems and addressing various control weaknesses in operational and management procedures) is part preventive and part corrective action.” [3]

This standard is a multipart standard and handled with 2 titles.

- “ISO/IEC 27035-1:2016 Principles of incident management” [9]
- “ISO/IEC 27035-2:2016 Guidelines to plan and prepare for incident response (Plan and Prepare, Lessons Learned)” [9]

### **2.7.27 “ISO/IEC 27036 Information security for supplier relationships” [9]**

“ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information risks involved in the acquisition of goods and services from suppliers. The implied context is business-to-business relationships, rather than retailing, and information-related products. The terms acquisition and acquirer are used rather than purchase and purchasing since the process and the risks are much the same whether or not the transactions are commercial (e.g. one part of an organization

or group may acquire products from another part as an internal transfer without literally paying for them).” [3] The parts are;

- “ISO/IEC 27036-1:2014 - Information security for supplier relationships - Part 1: Overview and concepts” [9]
- “ISO/IEC 27036-2:2014 - Information security for supplier relationships - Part 2: Requirements” [9]
- “ISO/IEC 27036-3:2013 - Information security for supplier relationships - Part 3:- Guidelines for ICT supply chain security” [9]
- “ISO/IEC 27036-4:2016 - Guidelines for security of cloud services” [9]

#### **2.7.28 “ISO/IEC 27037:2012 Guidelines for identification, collection and/or acquisition and preservation of digital evidence” [9]**

“ISO/IEC 27037:2012 provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions. ISO/IEC 27037:2012 gives guidance for the following devices and circumstances:

- Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions,
- Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,
- Mobile navigation systems,
- Digital still and video cameras (including CCTV),
- Standard computer with network connections,
- Networks based on TCP/IP and other digital protocols, and
- Devices with similar functions as above.” [9]

#### **2.7.29 “ISO/IEC 27038:2014 Specification for digital redaction” [9]**

“ISO/IEC 27038:2014 specifies characteristics of techniques for performing digital redaction on digital documents. It also specifies requirements for software redaction

tools and methods of testing that digital redaction has been securely completed. The standard formally defines redaction as “permanent removal of information within a document” where document is formally defined as “recorded information which can be treated as a unit”. The definitions are important because, in other contexts and general use, these terms often mean other things ... and indeed later in the standard, redaction is expanded to include not just the removal of confidential content but also, if appropriate, indicating where content has been removed.

Even though this standard has a restricted scope, the risks it covers are significant and many of the associated controls are technically and procedurally complex. Like other ISO27000 series standards, it does not attempt to cover all the vagaries of the redaction process in great detail but provides sound if rather generic and high-level guidance.” [3]

### **2.7.30 “ISO/IEC 27039:2015 Selection, deployment and operations of Intrusion Detection [and Prevention] Systems (IDPS)” [9]**

“ISO/IEC 27039:2015 provides guidelines to assist organizations in preparing to deploy intrusion detection and prevention systems (IDPS). In particular, it addresses the selection, deployment, and operations of IDPS. It also provides background information from which these guidelines are derived. The standard is, in effect, an ISPS implementation guide and advisory.” [3]

### **2.7.31 “ISO/IEC 27040:2015 Storage security” [9]**

“ISO/IEC 27040:2015 provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use. ISO/IEC

27040:2015 provides an overview of storage security concepts and related definitions. It includes guidance on the threat, design, and control aspects associated with typical storage scenarios and storage technology areas. In addition, it provides references to other International Standards and technical reports that address existing practices and techniques that can be applied to storage security.” [9]

### **2.7.32 “ISO/IEC 27041:2015 Guidance on assuring suitability and adequacy of incident investigative methods” [9]**

“The primary focus of this standard is on assurance for the forensics processes relating to investigation of digital evidence. Credibility, trustworthiness and integrity are fundamental requirements for all forensics methods: this standard promotes the assurance aspects of investigating digital evidence.

The standard offers guidance on assuring the suitability and adequacy of the methods for investigating digital forensic evidence. It describes methods through which all stages of the investigation process can be shown to be appropriate (proper and suitable in themselves, and correctly performed).

The standard “should be applied prior to any investigation, in the context of principles and processes (defined in ISO/IEC 27043) and sound preparation and planning (defined in ISO/IEC 27035-2) to assure the suitability of methods to be applied in the investigative processes described in ISO/IEC 27037 and ISO/IEC 27041.” [9]

### **2.7.33 “ISO/IEC 27042:2015 Guidelines for the analysis and interpretation of digital evidence” [9]**

“ISO/IEC 27042:2015 provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. It encapsulates best practice for selection, design, and implementation of analytical processes and recording sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.

ISO/IEC 27042:2015 provides a common framework, for the analytical and interpretational elements of information systems security incident handling, which can be used to assist in the implementation of new methods and provide a minimum common standard for digital evidence produced from such activities.” [9]

#### **2.7.34 “ISO/IEC 27043:2015 Incident investigation principles and processes” [9]**

“ISO/IEC 27043:2015 provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence. This includes processes from pre-incident preparation through investigation closure, as well as any general advice and caveats on such processes. The guidelines describe processes and principles applicable to various kinds of investigations, including, but not limited to, unauthorized access, data corruption, system crashes, or corporate breaches of information security, as well as any other digital investigation.” [3]

#### **2.7.35 “ISO/IEC 27050:2016 Electronic discovery” [9]**

“Electronic discovery is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding. ISO/IEC 27050:2016 is a multi-part standard offering an overview of electronic discovery and guidance for governance and management of electronic discovery. In addition, it defines related terms and describes the concepts, including, but not limited to, identification, preservation, collection, processing, review, analysis, and production of ESI. This standard also identifies other relevant standards (e.g. ISO/IEC 27037) and how they relate to, and interact with, electronic discovery activities. Here is the parts of this standard:

- ISO/IEC 27050-1:2016 Part 1: Overview and concepts
- ISO/IEC 27050-2 Part 2: Guidance for governance and management of electronic discovery (Draft)
- Part 3: Code of Practice for electronic discovery (Draft)

ISO/IEC 27050 is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities, and it is not intended to contradict or supersede local jurisdictional laws and regulations, so exercise care to ensure compliance with the prevailing jurisdictional requirements.” [9]

### **2.7.36 “ISO 27789:2013 Health informatics - Audit trails for electronic health records” [9]**

“ISO 27789:2013 specifies a common framework for audit trails for electronic health records (EHR), in terms of audit trigger events and audit data, to keep the complete set of personal health information auditable across information systems and domains. It is applicable to systems processing personal health information complying with ISO 27799. ISO 27789:2013 covers only actions performed on the EHR, which are governed by the access policy for the domain where the electronic health record resides. It does not deal with any personal health information from the electronic health record, other than identifiers, the audit record only containing links to EHR segments as defined by the governing access policy. It does not cover the specification and use of audit logs for system management and system security purposes, such as the detection of performance problems, application flaw, or support for a reconstruction of data, which are dealt with by general computer security standards such as ISO/IEC 15408-2.” [9]

### **2.7.37 “ISO 27799:2016 Health informatics - Information security management in health using ISO/IEC 27002” [9]**

“This standard offers guidance on information security management and information security controls in the context of the healthcare industry and medical organizations of various kinds - hospitals, labs, surgeries, medical insurers etc.

ISO 27799:2016 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

ISO 27799:2016 provides implementation guidance for the controls described in ISO/IEC 27002 and supplements them where necessary, so that they can be effectively used for managing health information security.

ISO 27799:2016 and ISO/IEC 27002 taken together define what is required in terms of information security in healthcare, they do not define how these requirements are to be met. That is to say, to the fullest extent possible, ISO 27799:2016 is technology-neutral. Neutrality with respect to implementing technologies is an important feature.” [9]

### **2.7.38 IN DEPTH OF ISO/IEC 27005/2011 [10]**

This International Standard provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements of ISMS according to ISO/IEC 27001. However, this International Standard does not provide any specific methodology for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector.

A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of ISMS.

This standard supports the concepts specified in ISO/IEC 27001 in generally and is designed to assist the implementation of information security management system based on a risk management approach.

It is a necessity to have a systematic approach to identify organizational needs of information security and manage information security risk management, also to create an effective information security management system.

Information security risk management in organizations must be a continual process to know about the risks and manage them. The process should help organizations to know their assets lists used in information processes, to know the vulnerabilities about them and threats using those vulnerabilities and threat the risks using a risk treatment plan to implement the recommendations and decisions using best practices, industry

solutions and personnel's experiences. Risk management analyses what are black holes while processing the information, what can happen using those black holes and what the possible consequences can be, before deciding what should be done and when, to reduce the risk to an acceptable level as stated *residual risk*.

It is stated in the standard [10] that information security risk management should contribute to the following;

- Risks being identified
- Risks being assessed in terms of their consequences to the business and the likelihood of their occurrence
- The likelihood and consequences of these risks being communicated and understood
- Priority order for risk treatment being established
- Priority for actions to reduce risks occurring
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring
- Risks and the risk management process being monitored and reviewed regularly
- Information being captured to improve the risk management approach
- Managers and staff being educated about the risks and the actions taken to mitigate them

After the assets lists which are used to process the information are identified, then the information security risk management process consists of context establishment, risk assessment, risk communication, risk review, risk treatment and risk acceptance and monitoring.



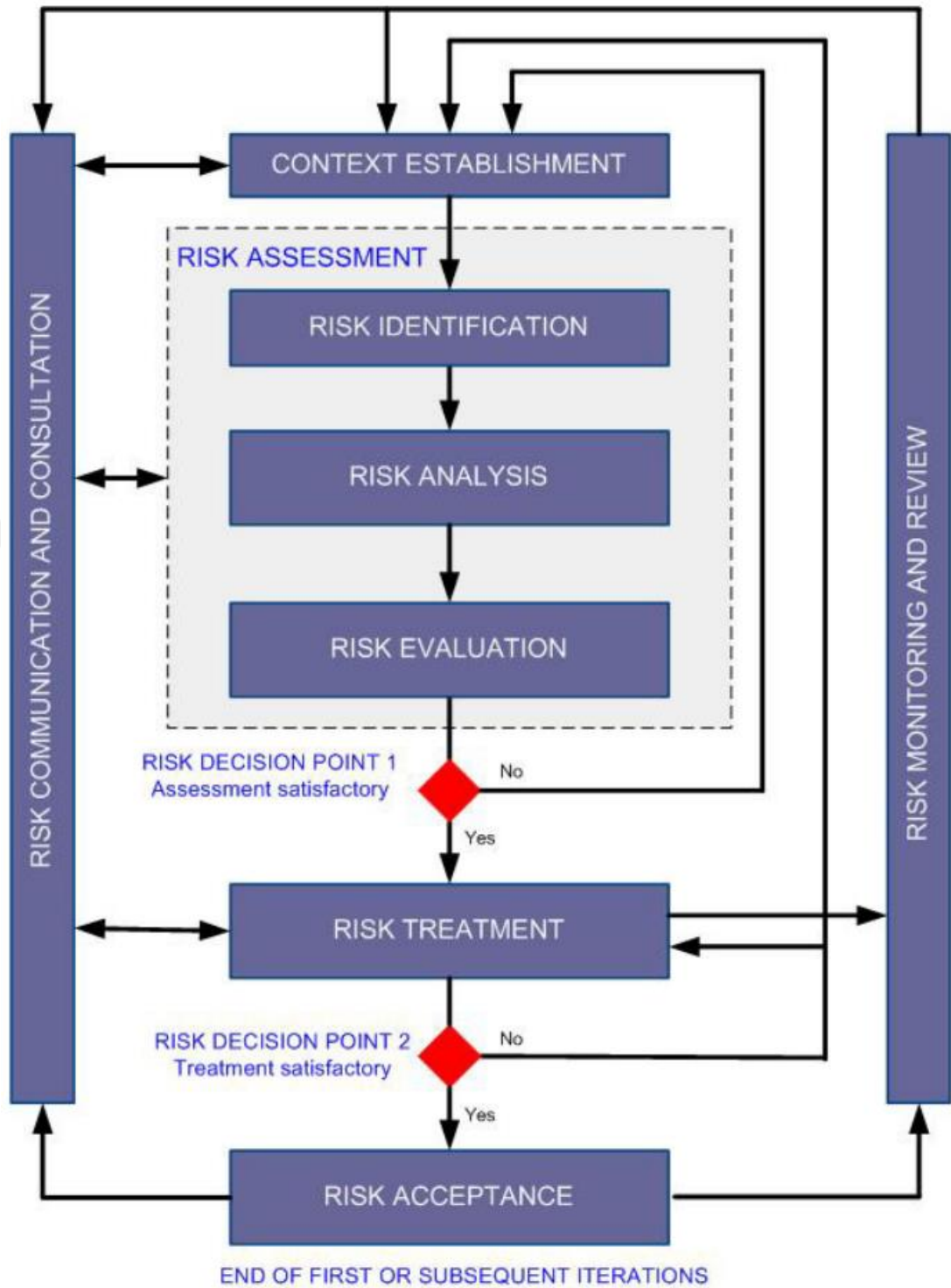


Figure 2.2 ISO/IEC 27005 Risk assessment process

Especially context establishment part includes personnel's experiences to make relations between assets and risks by analyzing business processes.

As Figure 2.2 illustrates, the information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach helps analysts to make risk assessment in depth of business process. That's a need because of rapid changes of business world. The iterative approach also provides review of the process and helps organizations to make improvements in processes.

The context is established after having the assets list of business process. Then a risk assessment is done. The first risk assessment may not include whole risks of the process. So that iterative approach is very useful. If this assessment provides enough information to define the action plans to reduce the risks to an acceptable level then the assessment task is completed and coming up step the risk treatment is started now. If the risk is at acceptable level, then we do not need to re-evaluate the risk means no need any iteration anymore. If not, another iteration of the risk assessment with revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) will be conducted, possibly on limited parts of the total scope (see Figure 2.2, Risk Decision Point 1).

The effectiveness of the risk treatment depends on the results of the risk assessment. It is possible that the risk treatment will not immediately lead to an acceptable level of residual risk. In this situation, another iteration of the risk assessment with changed context parameters (e.g. risk assessment, risk acceptance or impact criteria), if necessary, may be required, followed by further risk treatment (see Figure 2.2, Risk Decision Point 2).

When risk treatment plans are applied and risk assessment iterations are finished because of not being able to reduce more, then it is time to accept the residual risks. So that the risk acceptance activity is the dealing part of analysts and the managers of the organizations, because of there are only residual risks to evaluate and no iteration may be done more. This step is important where the implementation of controls is omitted or postponed, e.g. **due to cost**.

During the whole information security risk management process, it is important that communicating with the right staff and business managers to analyze risks and their treatment. After risk assessment step, information about identified risks can be very

valuable for the operational staff and managers to manage incidents and may help to reduce potential damage. The nature of ISO/IEC 27001 standard, risk awareness is so important to manage, mitigate the risks and the areas of concern to the organization assist in dealing with incidents and unexpected events in the most effective manner and first results of analysis are also important for operational staff and business managers to define risk treatment plans immediately and help the analysts to have less iterations. Every risk decision points in all steps must be documented and this would be helpful for iterative approach.

ISO/IEC 27001 based ISMS shall be risk based. The application of an information security risk management process defined here can satisfy this requirement. There are many approaches may be available to implement by the organizations. The organization should use whatever approach best suits their circumstances for each specific application of the process.

In an ISMS, the *plan* phase includes; establishing the context; risk assessment; developing risk treatment plan; risk acceptance; In the *do* phase, for reducing the risk implementing actions and controls using risk treatment plan to an acceptable level. In the *check* phase, risk assessment and risk treatment are determined by managers using the light of incidents and changes in circumstances. In the *act* phase, any actions including additional application of the information security risk management process required, are performed.

### 2.7.31.1 Plan-Do-Check-Act (PDCA) Model

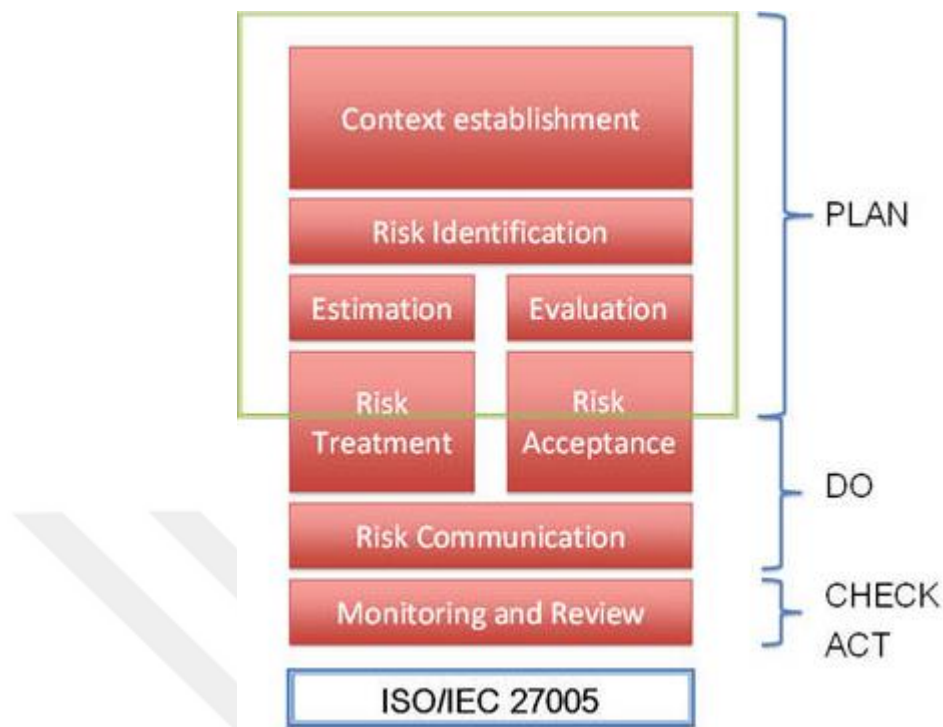


Figure 2.3 ISO/IEC 27005 PDCA Model [11]

As every ISO standard, ISO/IEC 27005 includes also PDCA Model. As seen Figure 2.3, risk identification, estimation of information security risk in terms of confidentiality, integrity and availability and evaluation of information security risk is grouped under *Plan*.

After planning and defining the information security risks and scoring the current value with a model then of course not all of information risks may be but information risks with **high scorings** must be under control. So that risk treatment plans or action plans must be defined and applied to reduce the scores. This stage is under *Do* section. At applying the action plans, in general it is expected to reduce the scores. This reducing may effect to other information security risks which are not in the same process group. Choosing a treatment activity is the most important to make the solution in the budget limits or with the minimum costing to the organization.

“It is essential to determine the purpose of the information security risk management as this affects the overall process and the context establishment in particular, this purpose can be:

- Supporting an ISMS
- Legal compliance and evidence of due diligence
- Preparation of a business continuity plan
- Preparation of an incident response plan
- Description of the information security requirements for a product, a service or a mechanism” [10]

In fact, risk management systems’ purposes are not defined above. A risk management framework may work standalone; all other system parts depend on risk assessment results. Executive management has no tolerance for adding those sorts of losses to the risk they already face so that compliance and due diligence are executed. Business continuity plans and incident response plans are created due to results of risk assessment process. We don’t agree the words written in standard above.

#### **2.7.31.2 Risk evaluation criteria**

Risk evaluation criteria should be developed for evaluating the organization's information security risk considering the followings:

- The strategic value of the business information process which is defined by personnel’s experiences
- The criticality of the information assets involved which is defined by personnel’s experiences
- Legal and regulatory requirements, and contractual obligations
- Operational and business importance of availability, confidentiality and integrity which is defined by personnel’s experiences
- Stakeholders expectations and perceptions, and negative consequences for goodwill and reputation

Additionally, risk evaluation criteria can be used to specify priorities for risk treatment which helps us to make an order about implementing the action plans to reduce the risks to acceptable level also.

As seen above, ISO/IEC 27005 information security risk management system uses personnel's experiences for;

- Defining the strategic value of the information is processed and due to this information value of the assets used in this process are also can be defined
- Defining the importance of information in terms of confidentiality, availability and integrity.
- Defining stakeholders' expectations.

To use this risk evaluation criteria defined in ISO/IEC 27005, it is good to have risk identification, risk estimation and risk evaluation with business process approach. With this approach, complete solution may become and implemented to organizations.

## CHAPTER 4

### COMBINING OF ALE MODEL BY LENSTRA and VOSS [1] APPROACH AND NEW MODEL

Of course in every organization, there is information defined as secret and also must be kept in safe from threats. In real life applications, every organization thinks that all information is secret for the outside of the world. Determining financial value of that information is more meaningful for the organizations to evaluate and applying action plans. To ensure value of the information, organizations have risk management systems to evaluate their risks within the information process. The risk management systems have analysis about risks to determine how to minimize the risks, with respect to a budget, of the *expected losses* about financial. “Although it is certainly relevant to know the expected losses, for capital management purposes it is also important to have accurate insight into the variability of the losses and in the Value at Risk (VaR), the probability that the losses exceed a given amount. But this more general quantitative approach (i.e., using more than just expected loss values) is not applicable in all situations. In the first place, it may be hard to collect so many data that the distribution functions can accurately be determined. This is in particular the case for so-called heavy-tailed distributions where high impact events occur with a very low probability; these typically occur in Information Security. It is illustrated by the observation that different organizations often select different distribution functions for the same types of events. Furthermore, collecting enough data to determine the distribution function underlying the behavior of certain IS threat is most likely impossible given the fast and constantly changing IS environment. From this point of view IS risk management is quite different from more traditional insurance and stock portfolio risk management.”

[1] The only need of risk management is for estimation of financial value of *expected losses* or not?

The *main question* may be “how much the estimation of financial value is true?”. Organizations may use Lestra and Voss approach [1] dealing with ALE model. As defined in *Chapter 1*, this model uses expected losses for threats about confidentiality, availability and integrity subjects. Also the model includes type of loss information and those two information have some scores which is defined by the experienced stuff in the organization who may evaluate those loss information dealing with the risks and know the business processes in the organization very well. Our model does not use those information but includes experienced stuff’s scoring information as information value and also includes financial values of the inventories effected by the risk, occurred by threats which uses vulnerabilities. These make model including quantitative values that can be used to make more quantitative risk management.

The creation of new model is based on real life information security management system implementation applications in telecommunication and manufacturing environments. There are legislative responsibilities for the telecommunication organizations because of creating or using lots of information in digital format. So the nature of the job, those types of organizations must use risk management methodologies to determine the right value of the information to keep in safe and use the budget more efficiently.

### **3.1 OBJECTIVES**

The main objective of this thesis is to come to a quantitative approach that helps with getting insight in and control over the defining information risks of an organization using financial information due to importance of meaning of cost controlling. The research objective is very broad in itself because of experiences may be differ from general experiences. That is why it needs to be placed in context, and constraints have to be specified, in order to give the research the right scope. In detail, the main goal will be to create an understanding of the applicability of quantitative models in information risk management by projecting a computational method on a generally used methodology for risk assessment similar to ISO/IEC 27005 and combining it with the financial values of the assets This will help the assessing organization in creating insight in the available gap and creates a possibility for the organization to have more



control over those gaps which create risks for business processes. Also organizations may have not only a qualitative method to implement risk assessment but also a quantitative method which deals more with the financial information of the assets in the processes to explain the loss of inventory easily to *top management*.

This research goal still leaves some room for interpretation because of information value is not still defined clearly by any company. Also to ensure that the research will be useful for the audience and achievable within the predefined time limits, specific research questions are specified (Section 3.2) and the new framework which includes ALE model and ISO/IEC 27005 framework is constructed (Section 3.3).

### 3.2 QUESTIONS

Risk management process has lots of problems in nature. Always asks when, why, who, which etc. At the analysis part, the most important things are;

- Defining the processes and steps,
- Defining the relations of process and communication routes,
- Defining the assets of the processes and owners of assets.

Those key findings help analysts to define the risk inventory and implementation areas of the solution in generally. In detail of course there are lots of information to be analyzed like responsibilities, management support, technology reviews etc.

After these reviews organizations should ask themselves about methodologies for defining risks. So the first question is;

- Which methodology helps me to define risks in an efficient way?

After choosing a method to define the risks, analysts want to have the model of scoring for identified risks, they are in doubt. Organizations behavior at scoring the information security risks depends only on personnel's experiences and Lenstra and Voss [1] approach also includes only that type of scoring defined as estimated loss and type of loss information. They may see different values for the defined risks. For example network specialists think that their switches and routers are so important to

keep in safe and because of the financial value, they must be in top class secure areas. But when analysts ask them about networking equipment like cables (CAT5, CAT6 etc.), they may think the risk is not so important, because they think there is no *unstructured technical* stuff even if their company is an ISP. So that there is a subjective evaluation of stuff and analysts may want to take into account both switches and other network equipment also. Of course, the experienced stuff who deals with business processes and information flow in the organizations must attend this step and give his/her ideas and scoring about information asset. In Lenstra and Voss [1] it is defined different and also in our model we include experienced staff's scoring also under different title. But estimating must be some rules to apply the model also and this is defined as risk assessment methodology and we have to choose one. So some other questions occur in mind like;

- How to select a suitable (qualitative) tool/methodology?

In which (qualitative) tools/methodologies for Risk Assessment exist and what are their characteristics, in what are currently often used (qualitative) methodologies for Risk Assessment and in what kind of information is concerned in *Information Risk Management*?

- How to select an applicable computational method?

In which computational methods for quantitative Risk Assessment exist and what are their characteristics and in what additional characteristics and/or requirements would a quantitative method need to have to make it practical and workable.

Also choosing qualitative methodology as we choose ISO/IEC 27005,

- How can we define values for confidentiality, availability and integrity?

To be clearer, let look at the meanings of confidentiality, availability and integrity definitions to define score in the right way.

### **3.2.1 Confidentiality**

“Confidentiality, being part of the concept of privacy, refers to preventing the unauthorized access, disclosure, and use of information or even the nature or existence of the information” [12].

“Only the individuals, processes or devices that are intended and authorized may have access to the data. Without appropriate controls, access or theft of information can be accomplished without a trace. Therefore, confidentiality is maintained through user authentication and access control. User authentication ensures that the person trying to access the data is authorized or not. Access control is the process of defining which users and groups should have access to the data. In short: Limited observation and disclosure of knowledge” [13].

### **3.2.2 Integrity**

Integrity is a somewhat broad phenomenon. In this case, it refers to the reliability and trustworthiness of the information in or produced by the information environment. Data integrity refers to the need to retain or preserve the information from source to destination. Source integrity refers to the verification process that is involved in ensuring that the data came from the correct source rather than from an imposter [14]. Integrity also refers to whether or not the correct data was initially entered, and whether the calculation or action will yield the same result each time.

“In short: Completeness, wholeness, and readability of information and quality of being unchanged from a previous state” [13].

### **3.2.3 Availability**

Because most companies rely heavily on computers and networks, and the data and information that reside within them, availability is a critical function. Companies have to be able to rely on electronic data and communications [15]. Availability defines the timely access to data, with timely defined in terms of functional significance. It is not possible to define timely as absolute because it depends on what the data is used for.

The above criteria can be used to describe many important security objectives and it is defined in ISO/IEC 27005 also. However, many people will have difficulties combining the security objective with criteria. Sometimes the objectives seem fitting to more criteria or even none at all. This makes the CIA model a good starting point for the young industries, but less applicable in the more mature industries. So this problem, mature industries use more information about assets to define the risk value close to reality. Those information may include possession information, location/utility information etc. In our real-life application you will see those type of information is handled also in the documentation.

So those questions, in our methodology, we used ISO/IEC 27000 series methodology which is defined in ISO/IEC 27005 Information Security Risk Management framework to define qualitative method for risk assessment. This framework defines analysts and experienced staff to score the inventory within defined rules. Also as a baseline model, we used ALE model and made some changes on that model declared later (Section 3.3). If we need to talk briefly about those modifications, adding financial value of inventory to the risk calculations using depreciation and salary information. Of course that information must be collected from related business units but in this thesis some assumptions may be used to calculate sample risk valuations.

### **3.3 NEW MODEL**

In Lenstra and Voss [1] approach for ALE model, there are estimations about confidentiality, availability and integrity losses defined in Table 1.1 and type of losses defined in Table 1.2 and combining those information together makes a value for information asset. At this point we have to use personnel's experiences. But using only those qualitative information including losses in confidentiality, availability and integrity domains are not enough for analysts to define the information security risk indicator quantitative. In real life examples which I'd been attended or managed, this part of the model comes into mind with the general experiences of stuff and using this experience is of course useful for the organization unless using different quantitative elements must be there for the organizations. Risk identification and scoring of its importance is a stage of risk assessment shown in Figure 2.3. After risk identification stage, it is good to estimate risks which may be occur and evaluate the risks are proper.

At this point we search within ISO series and there is no special model to have risk formula, only integrity, availability, confidentiality criterias to evaluate the assets value and the methodology defined in ISO/IEC 27005 also analyzed at Section 2.7.31 and those evaluations define a qualitative method as declared before. In our model, to define value we add some quantitative values to risk indicator formulas. Also risk assessment methodology is deal with general experiences which is scaled between very important and unnecessary. But ISO 27000 series, there is a qualitative methodology.

It is considered that a process based approach may be more useful to have a workaround for objective way of quantitative risk management of information security. Because while evaluating the assets in standalone, the main aim of the asset usage in a process and other assets in this process may be forgotten or defining a value for an asset with only itself is not a way of nature of the job. Thinking as a group of assets to make a business process helps analysts not to leave any space at risk identification stage. So that the analyst may find relations easily between assets and makes scoring better than other way that includes only one asset. But at process based approach, there is a big problem about the inventory list in the process. Due to nature of information technology domain there are more relations between processes than others. For example; an authentication system including MS Active Directory Server may be deal with some software inventories and also ERP system. Those relations cause a total effect on systems if any risk gives damage to authentication system and destroys it. So this total effect, every risk value or formulation may include MS Active Directory Server, licenses, operating system of hardware and licenses, hardware which runs operating systems' values. But at this point there is a loop. If calculation includes all the inventories in the process then some processes would become same value because they will include all inventories in the same way. But handling assets alone makes the analysis easier and the subject more manageable. In the model we developed, we use the financial value of the assets those are affected by the specified threat and salary information for spending time for the asset.

When we look into details the defined loss information in *Table 1.1* is calculated in different way with our model. We use financial value of the asset in risk indicator formula and man/day cost information also. When we analyze the formula defined in

Lenstra and Voss approach [1], we see *estimated loses* and *type of loses* terms about confidentiality, availability and integrity. Both of those are defined by the experienced staff and still this representation does not give us to determine the real financial effect of the risk on assets. But this determination looks similar importance values  $I_c(p)$ ,  $I_i(p)$ ,  $I_a(p)$  which we will use information values to substitute the loses. In our model we also need to define the importance value (values are like loss amount values) for confidentiality, availability and integrity titles with experienced staff who are deal with the business process and knows information flow in the organization, using ISO/IEC 27005 model. After scoring the importance values like loss values, scores are multiplied to define the assets total value. The definitions for the importance values of asset are shown *Table 3.1* below.

Symbol	Explanation
p	Business process
$I_c(p)$	Estimated importance of confidentiality for process p
$I_i(p)$	Estimated importance of integrity for process p
$I_a(p)$	Estimated importance of availability for process p

Table 3.1 Estimate importance values

Total importance value of asset “a” for process “p” is as;

$$I_a(p) = I_A(p) * I_I(p) * I_C(p)$$

Our formula for importance scoring is based on  $5 \geq \max (I_c(p), I_i(p), I_a(p)) \geq 1$  and  $I(p)$  for this three subjects must be integer assumption. This scale can be change by analysts but in general this scale is used. The maximum value of  $I_a(p)$  may be 125 in this scale and the minimum value may be only 1. So this assumption, we may only define the standard’s need about confidentiality, availability and integrity. ISO/IEC 27005 makes organizations to know about their information security risks, their

possibilities and damages caused by those risks. So that most of the organizations define the possibility of the risk of asset and damage of the risk elements by the experienced staff and that's the easy way to comply with the standard ISO/IEC 27001. At this point, we admit the Lenstra and Voss [1] approach's threat and skill level required for the threat. From this point of view, it will be clearer to happening of risk dependencies.

Still there is no financial information. Also current likelihood indicator of IS risk formula defined in Lenstra and Voss [1] approach on ALE model does not include quantitative notifications only based on some assumptions which is mentioned at *Chapter 1* before as loss amount and source of threat, access required for the threat and skill level require for the threat.

Now we apply those assumptions to formula below

$$P(t) = \text{Source}(t) * \text{Access}(t) * \text{Skill}(t) [1]$$

Also Lenstra and Voss [1] approach to ALE Model defines the current IS risk indicator as;

$$R_{cur}(p, t) = \max(T_c L_c(p), T_i L_i(p), T_a L_a(p)) P(t) [1]$$

Substitution for the element of  $\max(T_c L_c(p), T_i L_i(p), T_a L_a(p))$ , we assume the  $I_a(p)$  value which determines the importance value of asset  $a$  in process  $p$ . So this substitution, the formula becomes;

$$R_{cur}(p, t) = I_a(p) * P(t) [1]$$

$$I_a(p) = I_A(p) * I_I(p) * I_C(p)$$

Now our *current IS risk indicator*  $R_{cur}(p, t)$ , formula uses importance value of asset  $a$  in process  $p$ ,  $I_a(p)$  and *current likelihood indicator of risk*,  $P(t)$ .

The losses are defined for the Lenstra and Voss [1] approach to ALE model which do not include real financial information and only estimations of them used. To indicate this information quantitative in model, assume that financial value of an asset is  $F(a)$ , which  $a$  is asset's identification.

Financial value of an asset includes data from purchasing system as invoice prices and also man/day cost information which uses salary information and that information can be in hand from the purchasing system or the calculation of depreciation value from Accounts department of any company if it is a fixed asset and also salary information from HR department. By using this systematic information, our model would be integrated to company's information system also. For the fixed asset calculation and salary information calculation, first we have to know depreciation ratio of the asset to calculate fixed asset calculation. It is calculated as;

$$\text{Depreciation ratio} = \frac{1}{\text{Economical lifetime period}}$$

By using depreciation ratio which is given by Revenue Administration Department, Gelir İdaresi Başkanlığı [16], the depreciation value of an asset is calculated as;

$$\text{Depreciation value} = \text{Invoice value} * \text{Depreciation ratio}$$

<b>Symbol</b>	<b>Explanation</b>
DR (a)	Depreciation ratio of asset a [16]
E(a)	Economical lifetime period of asset a (is given by governmental institutions) [16]
D(a)	Depreciation value of asset for a year.

Table 3.2 Depreciation indicators

At the table above, invoice value is the value written on the purchasing invoice. Economical lifetime period and depreciation ratio is given by governmental institutions[16] . You have to find your assets' group in the list and get your depreciation ratio and economical lifetime for the asset.



Beside this calculation, man/day costing will included by the calculation. To make this calculation salary information must be get from related business unit and used. To calculate this; we may think of that a year has 52 weeks and every week has 2 days of weekends. This means;

$$\begin{aligned} \text{Workdays} &= 365 - (52*2) \\ &= 261 \text{ days} \end{aligned}$$

to work within the defined inventory and we will use this value for workdays count as standard. Also Monthly basis gross amount salary information must be multiplied by 12 to calculate yearly gross amount of a salary. Then division of the value with 261 days will give us the daily cost information. To calculate hourly gross amount then divide the daily value to daily work hours.

Lets say  $S$  is the salary for the responsible staff from process multiplied by 12 for year gross amount calculation for the process  $p$ , yearly periodic price either license or maintenance is  $Y$  for asset  $a$ , then *yearly financial value* is;

$$F(t) = S(a) + Y(a)$$

If there are another people for the asset and process then their salaries also must added to  $S(p)$  value.

In a whole management system which is built on information systems including special software, ERP systems, system management systems, security systems, we may get that information easily within the system integration. But to find such a system is not easy in real life conditions. So of that we will use the salary information which is defined at organization procedures. Also we are going to use assets' cost information like yearly depreciation value. According to Table 3.1, the yearly depreciation value of an asset is identified by is  $D(a)$ . But when calculating depreciation, we have to think about the investment not for yearly prices for example licenses. Yearly prices variable deals with the asset itself and it is evaluated together but salary information is not dealing with the asset's own. So it will be evaluated separately.  $Y(a)$  is a symbol for yearly paid price similar to *license price of inventory* whose price method is similar

that and services like *maintenance value*. If there is an old version product which is not priced per licenses anymore then yearly maintenance value of this asset is calculated from the *last license price* and it goes on like that up to scrapping of it. Our assumption about license values and maintenance values of those type of assets are 20% of list price.

If  $I$  is the set of assets which is affected by the threat  $t$  in process and if threat  $t$  effects more than one asset in the process then we have to include total value, so that calculation of all assets financial values for year,  $F(t)$  is as;

$$F(t) = S(a) + \sum_{a \in I} (D(a) + Y(a))$$

The total financial value of the process  $p$  for the threat  $t$ ,  $F_t(p)$  is shown as;

$$F_t(p) = P(t) * F(t)$$

Now we have new calculation of financial value of current likelihood IS risks financial value for the threat  $t$  of process  $p$  using yearly financial values.

After this financial value adding then the importance value like estimation of loss like in Lenstra and Voss [1] approach makes our model integrated with ISO/IEC 27005. Also including of  $P(t)$  makes our model integration with ISO/IEC 27005. By adding the importance value of asset  $a$  in process  $p$  which is defined by analyst and experienced staff, our formula becomes;

$$F_t(p) = P(t) * F(t) * I_a(p)$$

If we remember the formula about current IS risk indicator on *page 63*, then we may write down the formula as;

$$F_t(p) = R_{cur}(p, t) * F(t)$$

As a result we present the financial value of information security risk.

This model is totally different from Lenstra and Voss [1] approach to ALE model. It includes financial value from the depreciation calculation provided by accounting departments of the organization, salary information from relate business unit and also yearly prices for the asset. Also this formula uses Lenstra and Voss [1] approach including current likelihood indicator formula and uses it to comply the standard ISO/IEC 27001 and integrates this indicator formula within the probability of the threat. Using some assumptions about the values of skill, access and sources makes clearer about probability calculation of the information risk.

There are some difficulties about implementing new model as mentioned before. Because as mentioned at *Chapter 2 on page 18* there some assumptions about the possibility of risk appearance but again at the same place there is an option about experienced staff idea about this and user is allowed to change the value of  $P(t)$ , current likelihood indicator formula also user must change the value of  $P(t)$ .

Another implementation problem is about the getting financial value of the assets, man/day cost information and keeping them in secure. Organizations don't want all staff to know about purchasing prices and man/day costs. So that risk calculations or elements of this calculation must be kept in secure and only security analysts may see those values or calculation automation must be developed. Of course that's a *management decision* including the way of permit but this is a must for applying this model to real life and this will be a big step and the hard way of implementation.

## CHAPTER 5

### REAL LIFE APPLICATIONS WITH NEW MODEL

In this Chapter, we are going to apply our model to a real life ISMS application. Our sample is about an ISP organization which has millions of customers use the internet infrastructure of that company. This company has lots of branches in other cities and also in bigger cities like Ankara, İstanbul, İzmir, Bursa etc. it has more than one branch. It has different types of buildings; some of the for only management and public relations, some of them includes only technical stuff etc. Also there are different business units in the organizations and one of them is responsible about internet services in Turkey named as *Internet and Interactive Services Department (İVEİ)* and act as *Internet Service Provider*. Also some other business units like *Information Systems Department, Budget Control Department and Accounting Department* etc. have relations with İVEİ. So that organization has different types of information. But in our sample the scope includes only İVEİ unit and its operations at serving services. Just this scope also includes lots of information, other business unit relations and governmental relations to be managed. Due to this variety, there are different types or vulnerabilities and threats may use those vulnerabilities. This situation means lots of risks may be evaluated by the analysts and determining the scores of those information security risks needs a proper algorithm which would be more objective. Of course as we declared our new model at Section 3.3 and this model will be used to define the scores for the information security risks. In our sample we will implement our model to an asset's specific risk and its vulnerabilities and threats. Then we will install those sample value to developed software and we will see the usage of this software as a system.

## 4.1 Collected Information

To see this application first of all, we have to see the asset list of business processes. For our example İVEİ which department serves internet services to all over Turkey of a telecommunication company, it would be hard to have full of list in detail of course. The organization the first wants to implement and build up ISMS in systems' center which is located in Balgat district and also they defined the some assets at the city locations into the scope. Some assets also managed by other departments in the organization and for this situation, İVEİ uses service agreements to manage that equipment. When we look into detail into assets in the list shown at *Figure 4.1* on *page 72*, it includes physical assets those process the information and also used in internet services processes. The list also includes owner of the asset because there are different departments serving to ISP department as services in the organization. So this services this section in the list includes the department information.

The responsible group/person is defined at *Responsible of the asset* section. The responsible defined in this column manages, controls, changes and uses this asset unless defined differently in another document or list which is approved by the organization. Also this responsible people or group score the asset's value defined at *Asset's value* section with the information security analysts. Above the models mentioned as *experienced personnel* as we see, this column includes members of those experienced staff information.

The class/mission section is the group of the asset. This helps analysts about general grouping the assets for reporting easily.

Location column includes the location of the asset. As we mentioned above, organization's İVEİ locations and system center locations are defined at this column. Also there is location information like "Mobil". This asset is separated from others because of the risk assessment of this asset is different because of the mobility option creates more vulnerabilities may be used by treats.

Now one of the elements in the formula is defined at the *Asset's value* columns. These scores are given by the security analyst and experienced staff defined at the *Responsible of the asset* column in the list. This scoring is made for 3 different subjects

as confidentiality, availability and integrity which are mentioned at *ISO/IEC 27005 analysis* in *Section 2.7.31*. ISO/IEC 27005 wants analyst to analyze the asset in the matter of confidentiality, availability and integrity. These columns become together defined in mathematical formula and becomes as *importance value of asset*.

The last column in the list is for explanation about the assets.

Also organization's acceptable risk level is required us to compare the old new methods at least. Organization's acceptable risk level point,  $R_a$  is calculated like below;

$$R_a = \text{Asset value} * \text{Possibility value} * \text{Damage value}$$

Asset value is defined at the assets list document mentioned above. Possibility value and damage value is defined at risk documentation mentioned below *at page 77*.

Those values all are estimation of experienced stuff in the organization. Organization defined the acceptable level of risk as 243. To find out how to define this information, let's look at the tables below [17]. Analysts agreed on to use the middle scores to define acceptable level of the risk.

Gizlilik Değeri	Bütünlük Değeri	Erişilebilirlik Değeri	AÇIKLAMA
5	5	5	Çok Yüksek
4	4	4	Yüksek
3	3	3	Orta
2	2	2	Düşük
1	1	1	Çok Düşük

Table 4.1 Asset values of the organization

VARLIK DEĞERLERİ					
GÜVENLİK HEDEFİ	ÇOK DÜŞÜK	DÜŞÜK	ORTA	YÜKSEK	ÇOK YÜKSEK
<b>GİZLİLİK</b>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi açığa çıkmaz</u> . Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi açığa çıkmaz</u> . Açığa çıkan kritik seviyesi altındaki bilgi kurumu çok az etkiler. Etki <u>kısa vadede</u> telafi edilebilir.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi açığa çıkmaz</u> . Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkiler. Etki <u>orta vadede</u> telafi edilebilir.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi açığa çıkar</u> . Açığa çıkan kritik bilgi kurumu etkiler. Etki <u>orta vadede</u> telafi edilebilir.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi açığa çıkar</u> . Açığa çıkan kritik bilgi kurumu etkiler. Etki <u>uzun vadede</u> telafi edilebilir.
<b>BÜTÜNLÜK</b>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi kontrol dışı değişmez</u> . Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi kontrol dışı değişmez</u> . Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu çok az etkiler. Etki <u>kısa vadede</u> telafi edilebilir.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi kontrol dışı değişmez</u> . Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkiler. Etki <u>orta vadede</u> telafi edilebilir.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi kontrol dışı değişir</u> . Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki <u>orta vadede</u> telafi edilebilir.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi kontrol dışı değişir</u> . Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki <u>uzun vadede</u> telafi edilebilir.
<b>ERİŞİLEBİLİRLİK</b>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgiye erişilebilir</u> . Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgiye erişilebilir</u> . Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu çok az etkiler. Etki <u>kısa vadede</u> telafi edilebilir.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgiye erişilebilir</u> . Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkiler. Etki <u>orta vadede</u> telafi edilebilir.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgiye erişilemez</u> . Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki <u>orta vadede</u> telafi edilebilir.	Varlığa bir zarar gelmesi durumunda <u>kritik bilgiye erişilemez</u> . Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki <u>uzun vadede</u> telafi edilebilir.

Table 4.2 Asset values matching table with CIA

OLASILIK DERECESESİ	OLASILIK	AÇIKLAMA
5	Çok Yüksek	Tehdit kaçınılmazdır
4	Yüksek	Tehdit sıkça tekrarlanır
3	Orta	Tehdit gerçekleşebilir
2	Düşük	Tehdit nadiren gerçekleşir
1	Çok Düşük	Tehdit yok denecek kadar

Table 4.3 Possibility values of risks

HASAR DERECESESİ	HASAR	AÇIKLAMA
5	Çok Yüksek	Kurumsal sürekliliği tehlikeye sokacak hasar
4	Yüksek	Faaliyeti itibar kaybına yol açacak kadar kesintiye uğratabilecek hasar
3	Orta	Faaliyeti önemsiz ölçüde kesintiye uğratabilecek hasar
2	Düşük	Faaliyeti etkileyen ama kesintiye uğratmayan hasar
1	Çok Düşük	Faaliyeti doğrudan etkilemeyen hasar

Table 4.4 Damage values of risks to assets

No	Varlık Sahibi	Varlık Sorumlusu	Sınıf / Görevi	Yeri / Konumu	Varlık Değeri			Açıklama	
					Gizlilik	Bütünlük	Erişilebilirlik		
					Sonuç Değeri				
					G	B	E		
1	ISS Bölümü	Sistem Grubu	Sunucu	İstanbul Merkezli Müdürlüğü	4	4	3	48	İnternetim abonelerine DNS hizmetinin verilmesi (2.Adet)
2	ISS Bölümü	Sistem Grubu	Sunucu		4	4	3	48	İnternetim abonelerine uzantılı mail hizmetinin verilmesi (1Adet)
3	ISS Bölümü	Ağ Grubu	Ağ Güvenlik Cihazı		4	3	4	48	İl Müdürlikleri ve İl Müdürlükleri aarsı güvenli ağ alt yapısının sağlanması (1.Adet)
4	ISS Bölümü	Sistem Grubu	Sunucu		3	4	2	24	Sunucu ve ağ cihazlarının izlenmesi (1.Adet)
5	ISS Bölümü	Sistem Grubu	Sunucu		2	4	4	32	CNR, TIB ve AAA sunucu için sanallaştırma sunucusu (2.Adet)
6	ISS Bölümü	Ağ Grubu	Sunucu	İl Müdürlikleri	3	4	4	48	Yetkilendirme sunucusu (2.Adet)
7	ISS Bölümü	Ağ Grubu	Ağ Cihazı	İl Müdürlikleri	3	4	4	48	sonlandırma Cihazı (35.Adet)
8	ISS Bölümü	Ağ Grubu	Ağ Güvenlik Cihazı	İl Müdürlikleri	4	4	3	48	Güvenli İnternet Hizmeti Cihazı (35.Adet)
9	ISS Bölümü	Ağ Grubu	Ağ Cihazı		2	4	4	32	Anahtar Cihazlar (3.Adet)
10	ISS Bölümü	Ağ Grubu	Ağ Cihazı	İl Müdürlikleri	3	4	4	48	Anahtar Cihazlar
11	ISS Bölümü	Ağ Grubu	Ağ Cihazı	İl Müdürlikleri	3	4	4	48	İleri Yön Sinyali Modülatörü
12	ISS Bölümü	Ağ Grubu	Ağ Cihazı	İl Müdürlikleri	3	4	4	48	İleri Yön Sinyali Modülatörü

Figure 4.1 Physical Assets List



No	Varlık Sahibi	Varlık Sorumlusu	Sınıfı / Görevi	Yeri / Konumu	Varlık Değeri					Açıklama
					Gizlilik	Bütünlük	Erişilebilirlik	G * B * E	Sonuç Değeri	
13	ISS Bölümü	Sistem Grubu	Sunucu	[Redacted]	4	3	4	48	Veri Depolama Ünitesi (1 Adet)	
14	ISS Bölümü	Tüm Birim	Ağ Cihazı	[Redacted]	4	2	3	24	masa üstü telefonlar	
15	ISS Bölümü	Tüm Birim	Ağ Cihazı	[Redacted]	2	4	3	24	USB-DVD	
16	ISS Bölümü	Tüm Birim	Ağ Cihazı	[Redacted]	2	4	3	24		
17	ISS Bölümü	Sistem Ve Ağ Grubu	Sistem Odası	[Redacted]	5	5	3	75		
18	BT Altyapı ve Sistem Yönetimi Direktörlüğü	Sistem Ve Ağ Grubu	Personel Çalışma Ekipmanı	Mobil	3	4	3	36		
19	ISS Bölümü	Ağ Grubu	Ağ Cihazı	İl Müdürlükleri	2	3	3	18		
20	Yedekleme Ünitesi	Sistem Grubu	Sunucu	[Redacted]	3	2	2	12	Yedek verileri kasete aktarmak için	
21	Yedekleme Sunucusu	Sistem Grubu	Sunucu	[Redacted]	3	3	2	18		
22	Fiber Kanal Anahtarı	Ağ Grubu	Ağ Cihazı	[Redacted]	1	4	3	12	Sunucular arası anahtarlama cihazı	
23	Merkezi Veri Depolama Sistemi	Sistem Grubu	Sunucu	[Redacted]	4	4	2	32		
24	Dosya Depolama Sunucusu	Sistem Grubu	Sunucu	[Redacted]	5	3	2	30	Ortak Dosya Sunucu	

Figure 4.1 Physical Assets List (continued)

No	Varlık	Varlık Sahibi Varlık Sorumlusu Sınıfı / Görevi			Yeri / Konumu	Varlık Değeri			Sonuç Değeri	Model / Sürüm Açıklama
		ISS Bölümü	Sistem Grubu	Microsoft İşletim Sistemi		Gizlilik	Bütünlük	Erişilebilirlik		
1	Sunucu İşletim Sistemleri	ISS Bölümü	Sistem Grubu	Microsoft İşletim Sistemi	[Redacted]	2	4	1	8	Microsoft 2003/2008
2	Sanal Sunucu yazılımı	ISS Bölümü	Sistem Grubu	İşletim Sistemi	[Redacted]	3	4	1	12	Vmware ESX 3.5 yazılımları
3	Abone yetkilendirme yazılımları	ISS Bölümü	Sistem Grubu	Uygulama Yazılımı	[Redacted] Müdürlükleri	3	4	1	12	Cisco Network Registrar yazılımları
4	E-posta sunucu yazılımı	ISS Bölümü	Sistem Grubu	Uygulama Yazılımı	[Redacted]	4	4	1	16	IceWarp Merak Mail Server 10
5	AAA yazılımı	ISS Bölümü	Sistem Grubu	Uygulama Yazılımı	[Redacted]	4	2	1	8	Cisco Secure ACS 4.2
6	Network Monitoring Sistemi	ISS Bölümü	Sistem Grubu	Uygulama Yazılımı	[Redacted]	4	3	1	12	Cacti
7	Yönlendirici işletim sistemi	ISS Bölümü	Ağ Grubu	IOS	II Müdürlükleri	2	4	1	8	Cisco CMTS IOS
8	Güvenlik sistemleri yazılımları	ISS Bölümü	Ağ Grubu	OS	II Müdürlükleri	5	3	1	15	Astaro Security Gateway yazılımları
9	DNS Servisi	ISS Bölümü	Ağ Grubu	Servis Yazılımı	[Redacted]	4	3	1	12	Microsoft 2003
10	Yazıcı yazılımları	ISS Bölümü	BT Altyapı ve Sistem Yönetimi Direktörlüğü	Servis Yazılımı	[Redacted]	2	1	2	4	HP
11	Veri Depolama Servisi	ISS Bölümü	Sistem Grubu	Servis Yazılımı	[Redacted]	5	3	3	45	Microsoft 2003
12	Astaro Monitoring Yazılımı	ISS Bölümü	Ağ Grubu	Uygulama Yazılımı	[Redacted]	2	2	2	8	Astaro
13	Yedek Alma Yazılımı	ISS Bölümü	Sistem Grubu	Uygulama Yazılımı	[Redacted]	3	3	2	18	Symantec
14	Yedekleme Sistemi Domain Kontrol Servisi	ISS Bölümü	Sistem Grubu	Servis Yazılımı	[Redacted]	2	2	2	8	
15	Merkezi Veri Depolama Sistemi Yönetim Programı	ISS Bölümü	Sistem Grubu	Uygulama Yazılımı	[Redacted]	4	3	2	24	Hitachi SAN

Figure 4.2 Software Assets List

No	Varlık Sahibi	Varlık Sorumlusu	Sınıf / Görevi	Yeri / Konumu	Bulunduğu ortam	Bilgiyi İşleyen Yazılımlar	Bilgiyi İşleyen Donanımlar	Bilgiye Erişen Taraflar / Kişiler	Varlık Değeri	Sonuç Değeri	Açık	
								Gizlilik	Bütünlük	Erişilebilirlik	G * B * E	
1	ISS Bölümü	Satın Alma Grubu	Doküman / Sözleşme		Basılı doküman	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	3	2	4	24
4	ISS Bölümü	Ağ Grubu	Doküman / Form	Yönetim Sistemi	Basılı doküman	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	2	2	2	8
5	ISS Bölümü	Tüm Birim	Doküman / Kalite Planı	Yönetim Sistemi	Elektronik olarak	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	4	3	4	48
6	ISS Bölümü	Ağ Grubu	Doküman / Form	Yönetim Sistemi	Basılı doküman	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	2	2	2	8
7	ISS Bölümü	Ağ Grubu	Doküman / Form	Yönetim Sistemi	Basılı doküman	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	2	2	2	8
8	ISS Bölümü	Ağ Grubu	Doküman / Form	Yönetim Sistemi	Basılı doküman	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	2	2	2	8
9	ISS Bölümü	Ağ Grubu	Doküman / Topoloji		Elektronik olarak	Microsoft Office Visio	ISS Bölümü Personeli	ISS Bölümü Personeli	2	1	2	4
10	ISS Bölümü	Ağ Grubu	Doküman / Envanter		Elektronik olarak	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	2	1	2	4
11	ISS Bölümü	Tüm Birim	Doküman		Elektronik olarak	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	4	3	2	24
12	ISS Bölümü	Tüm Birim	Doküman		Elektronik ve Basılı olarak	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	3	2	3	18
13	ISS Bölümü	Tüm Birim	Doküman		Elektronik ve Basılı olarak	Microsoft Office	ISS Bölümü Personeli	ISS Bölümü Personeli	3	2	3	18

Figure 4.3 Information Assets List

Varlık Sorumlusu	Sınıf / Görevi	Yeri / Konumu	Varlık Değeri			Sonuç Değeri	
			Gizlilik	Bütünlük	Erişilebilirlik		
			G	B	E	Açıklama	
İnsan Kaynakları	Yönetici		3	4	4	48	
Direktör	Ağ Yönetim ve İşletimi Grubu		3	4	5	60	
Direktör	Sistem Yönetim ve İşletimi Grubu		3	4	5	60	
Direktör	Satınalma Grubu		3	4	5	60	
Direktör	BGYS Grubu		3	4	5	60	

Figure 4.4 Human Resources Assets List






No	Varlık	Varlık Sahibi	Varlık Sorumlusu	Sınıf / Görevi	Yeri / Konumu	Varlık Değeri			Sonuç Değeri		
						Gizlilik	Bütünlük	Erişilebilirlik	G	B	E
1	Bilgi İşlem Varklıkları için Teknik Destek Alınması	ISS Bölümü	BT Altyapı ve Sistem Yönetimi Direktörlüğü	Bilgi İşlem Servisleri		2	3	3	18		
2	Domain Hizmetinin Alınması	ISS Bölümü	BT Altyapı ve Sistem Yönetimi Direktörlüğü	Bilgi İşlem Servisleri		2	4	4	32		
3	Antivirüs Hizmetinin Alınması	ISS Bölümü	BT Altyapı ve Sistem Yönetimi Direktörlüğü	Bilgi İşlem Servisleri		2	4	4	32		
4	E-Posta Hizmetinin Alınması	ISS Bölümü	BT Altyapı ve Sistem Yönetimi Direktörlüğü	Bilgi İşlem Servisleri		4	4	4	64		
5	Kullanıcı Aktivitelerinin Loglarının Tutulması Hizmetinin Alınması	ISS Bölümü	BT Altyapı ve Sistem Yönetimi Direktörlüğü	Bilgi İşlem Servisleri		5	5	5	125		
6	Yama Raporlama Hizmetinin Alınması	ISS Bölümü	BT Altyapı ve Sistem Yönetimi Direktörlüğü	Bilgi İşlem Servisleri		2	4	4	32		
7	Yazılım Geliştirme Hizmetinin Alınması	ISS Bölümü	PYYGD	Yazılım geliştirme		4	5	5	100		IP Log Arayüzü
8	Sistemlerin Enerji Beslemesi Hizmetinin Alınması	ISS Bölümü	BİNA TESİSLER	Fiziksel Güvenlik		2	4	5	40		
9	Yangından Korunma Hizmetinin Alınması	ISS Bölümü	BİNA TESİSLER	Fiziksel Güvenlik		2	4	5	40		
10	Fiziksel Güvenlik Hizmetinin Alınması	ISS Bölümü	İDARI VE SOSYAL İŞLER	Fiziksel Güvenlik		2	4	5	40		
11	Temizlik Hizmetinin Alınması	ISS Bölümü	İDARI VE SOSYAL İŞLER	Temizlik		2	2	5	20		
12	Sistemlerin Soğutma Gereksinimi Hizmetinin Alınması	ISS Bölümü	BİNA TESİSLER	Fiziksel Güvenlik		2	4	5	40		
13	E-Posta Veya Telefon İle İli Müdürlüklerine Teknik Destek Hizmetlerinin Verilmesi	ISS Bölümü	Sistem / Ağ Grubu	İnternet Servis Sağlayıcı Hizmeti		2	3	4	24		İli müdürlüklerinden telefon veya e-mail yoluyla gelen problem ve önerilerin değerlendirilmesidir.
14	E-Posta Veya Telefon İle Çağrı Merkezi Ve Teşerünlara Teknik Destek Hizmetlerinin Verilmesi	ISS Bölümü	Sistem / Ağ Grubu	İnternet Servis Sağlayıcı Hizmeti		2	4	4	32		Çağrı merkezi, taşeron ofis telefon veya e-mail yoluyla gelen problem ve önerilerin değerlendirilmesidir.
15	Yasal Düzenleyici Faaliyetler	ISS Bölümü	Sistem / Ağ Grubu	İnternet Servis Sağlayıcı Hizmeti		5	4	3	60		TİB ve mahkeme karar ile gelen web adresi erişim engelleme kararlarının
17	 Stok İşlemleri Hizmeti	ISS Bölümü	Sistem / Ağ Grubu	İnternet Servis Sağlayıcı Hizmeti		1	2	1	2		

Figure 4.5 Services Assets List

## 4.2 Importance values definition

In *Section 3.3.1* at *Table 3.1* it is assumed that maximum value of importance of asset in the matter of those three subjects is 5.

$$I_a(p) = I_A(p) * I_I(p) * I_C(p)$$

So that calculation, *maximum* value of importance of asset may be;

$$I_a(p) = 5 * 5 * 5 = 125$$

So that calculation, *minimum* value of importance of asset may be;

$$I_a(p) = 1 * 1 * 1 = 1$$

So the scale is;

$$125 \geq I_a(p) \geq 1$$

We choose an example asset as “Operations Systems of Servers” numbered as 1 from software assets list to apply that model. This part complies with the ISO/IEC 27005. Its asset value is described in 3 titles as confidentiality, availability and integrity. Those points are given by the experienced staff at the organization with the security analyst. The points are;

Type	Score
Confidentiality	2
Integrity	4
Availability	1

Table 4.1 Sample asset’s importance values

With our model asset’s importance value  $I_a(p)$  is calculated as;

$$I_a(p) = 2 * 4 * 1 = 8$$

### 4.3 Current likelihood indicator calculation

To calculate current likelihood indicator, we have to use the list of assets' vulnerabilities, threats dealing with those vulnerabilities and risks occurred by those threats. At Figure 4.6 you may see the part of the list which includes our sample asset's desired information.

NO	VARLIK	VARLIK DEĞERİ	RISK	ZAAFIYET	TEHDİT	Kontroller uygulamadan önce			KONTROLLER
						I.O. OLASILIĞI	HASAR DERECEŚİ	RISK DEĞERİ	
1	Sunucu İşletim Sistemleri	8	İşletim sisteminin hizmet verememesi	Yetkin olmayan personel Güvenirdiği olmayan yazılım	Kullanıcı hatası Yazılım Sorunu	1	3	24	Erişim kısıtlaması yapılacaktır. Zararlı yazılardan korunma talimatı yazılacaktır.
				Yetersiz ağ güvenliği	Saldırı	1	3	24	İşletim sistemi güvenlik talimatı yazılacaktır. Ayrıca Ağ güvenlik cihazı ile korunmaktadır.
				Ağ erişim sorunu	Cihazın bağlandıđı, ağda problem	2	4	64	Sunucu trafiđini monitor edilecektir.
				Güncel olmayan sürümler	Zararlı yazılımların bozucu etkileri	1	2	16	Zararlı yazılardan korunma talimatı yazılacaktır.
				Yanıt yapılandırma	Hizmetlerin dođru çalıřmaması	1	3	24	İşletim Sistemlerinin nasıl yapılandırılacağı ile ilgili talimat yazılacaktır.
2	Sanallařtırma Sunucuları yazılımı	12	Sanal sunucular üzerinden sağlanan hizmetlerin durması	Yetkin olmayan personel Güvenirdiği olmayan yazılım	Kullanıcı hatası Yazılım Sorunu	1	4	48	Erişim kısıtlaması yapılacaktır. Zararlı yazılardan korunma talimatı yazılacaktır.
				Yetersiz ağ güvenliği	Saldırı	1	4	48	Ağ güvenlik cihazı ile korunmaktadır.
				Ağ erişim sorunu	Cihazın bağlandıđı, ağda problem	3	4	144	Sunucu trafiđini monitor edilecektir.
				Güncel olmayan sürümler	Zararlı yazılımların bozucu etkileri	1	2	24	Zararlı yazılardan korunma talimatı yazılacaktır.
				Yanıt yapılandırma	Hizmetlerin dođru çalıřmaması	2	3	72	Sanallařtırma sunucusunun nasıl yapılandırılacağı ile ilgili talimat yazılacaktır.
3	Abone yetkilendirme varlımları	12	Abonelerin internet erişimlerinin	Yetkin olmayan personel	Kullanıcı hatası	1	3	36	Erişim kısıtlaması yapılacaktır.

Figure 4.6 Software assets' risks

Defined risk is “The operating system is unable to serve” the threats and vulnerabilities are shown below at Table 4.2:

<b>Vulnerability</b>	<b>Threat</b>	<b>Total Probability to happen</b>	<b>Damage Score</b>	<b>Importance score</b>	<b>Risk Value</b>
Ability of system administrator	User error	1	3	8	24
Software security	Problem at software	1	3	8	24
Insufficient network security	Hacking	2	4	8	64
Network access error	Problem within the network used by	1	2	8	16
Old versions	Disruptive effects of malware	1	3	8	24
Wrong configuration	Services cannot work correctly	1	3	8	24

Table 4.2 Risk scores of example risk “The operating system is unable to serve” for sample asset

This calculation is so simple and complies with standard also. But with the assumption defined at Lenstra and Voss [1] approach to ALE Model we may make formula more accurate and detailed also.

Now let’s remember the calculation of Skill, Access and Source of threat then apply to our sample.



- “**Source of threat**, with two possible choices indicating, if the threat comes from a party *external* ( $Source(t) = 1$ ) or internal ( $Source(t) = 0,8$ ) to the company.” [1]
- “**Access required for the threat**, with two possible choices indicating if remote access ( $Access(t) = 1$ ) suffices to realize the threat or if local access ( $Access(t) = 0.6$ ) is required.” [1]
- “**Skill level required for the threat**, with four possible choices indicating the least level of skill required to realize the threat:
  - unstructured nontechnical ( $Skill(t) = 1$ );
  - unstructured technical ( $Skill(t) = 0.9$ );
  - structured nontechnical ( $Skill(t) = 0.75$ );
  - structured technical ( $Skill(t) = 0.25$ ).” [1]

We understand that the minimum value of current likelihood indicator  $P(t)$  may be;

$$P(t) = 0,8 * 0,6 * 0,25 \Rightarrow 0,12$$

and the maximum may be  $P(t) = 1 * 1 * 1 \Rightarrow 1$ . Minimum  $P(t)$  means low possibility. Due to these calculations  $P(t)$  scale is;

$$1 \geq P(t) \geq 0,12$$

As we mentioned our sample asset is “Operations Systems of Servers” at software assets list and first risk defined in risks inventory is “The operating system is unable to serve”. The first vulnerability shown in *Table 4.2* which includes vulnerabilities and threats of this risk is “Unauthorized person” and threat is “User error”. At the table the probability is given as 1 point over 5 and this means it has a low possibility to happen. When we adapt this to our model;

- Skill level required for threat; *structured technical* person may can do this threat so that  $Skill(t)$  equals 0,25.

- Access required for the threat; may be both inside and outside of the organization. So that  $Access(t)$  equals 1. This score is defined because of the possibility of happening the highest score is chosen
- Source of the threat; may be both internal and external. Because of possibility of the worst as external then  $Source(t)$  equals 1.

After this adaption then the formula of current likelihood which is substitution for possibility at the risks inventory table as *Table 4.2* is as;

$$P(t) = Source(t) * Access(t) * Skill(t) \quad [1]$$

$$P(t) = 1 * 1 * 0,25 \Rightarrow P(t) = 0,25$$

This value is substitution for the possibility column also as we mentioned  $I_a(p)$ , importance value defined in *Chapter 3* which can be defined by the experienced stuff.

We have the importance value in hand for “Operations Systems of Servers” as calculated;

$$I_a(p) = 8$$

As in our model, current IS risk indicator formula is;

$$R_{cur}(p, t) = P(t) * I_a(p)$$

$$= 8 * 0,25$$

$$R_{cur}(p, t) = 2$$

#### **4.4 Calculation of assets' financial value using new model**

As stated in *Chapter 3*, we used financial value of asset in the formula of current likelihood indicator. Now we have to find the financial value of the asset with two members in the list as depreciation value and man/day costing information. Now let's calculate the depreciation value. First of all we need to find the operating systems and their prices. This information may be collected from Microsoft dealers. In assets list it

is written like Windows Server 2003 and 2008. In fact we have to get prices from the invoices but for now we use pricegrabber's price list [18]. So that we may use

- Microsoft Windows Server 2003 R2 Enterprise Edition with Service Pack 2 - Complete Product price as \$3999 [18] and Microsoft Windows Server 2003 Terminal Server – License for each is \$84,99 [18] and there 5 people working at department so that terminal licenses' total value is \$424,95 .
- Microsoft Windows Server 2008 R2 Enterprise - 64-bit price is \$3400 [18] and price for one Microsoft Windows Server 2008 Terminal Services license is \$80,97 [18]. For 5 people working in department who may use the systems then price is \$404,85.

Now total price for Windows Server 2008 is \$3804,85 and total price for Windows Server 2003 is \$4423,95.

Now we have found yearly values, depreciation ratio and value for the asset. From Revenue Administration Department, Gelir İdaresi Başkanlığı, web site [16] we may see the software depreciation ratio as 33,33% and this means depreciation finishes at 3 years. For our samples all Windows Server 2003 and 2008 economic lifetime is over and from the model defined in Chapter 3, we have to use the license or maintenance prices. Both of them have same calculation and declared at *page 66*. So that yearly prices are;

For Windows 2003 Server;  $Y(a) = 424,95 * 0,2 = \$84,99$

For Windows 2008 Server  $Y(a) = 404,85 * 0,2 = \$80,97$

This calculation include only yearly price and only for one package. We will now calculate the salary information and sum them to have yearly financial information on hand.

In our sample, department includes 5 people and salaries is defined in the procedures as 4 of them have 3500TL monthly basis and one of them has 7000TL monthly basis which is manager. When calculating, we may use system administrator's salary information in relation with spending time information on the system in a month. So this scale, we will use 3500TL for salary information.

System administrator told that at normal conditions, he manages and monitors the system 5 hours in a week. This means his time spent on the asset “Server Operating Systems”; 5 hours \* 52 weeks in a year => 260 hours spent. There are 9 hours in a day as working hours as organization rule. That means 260/9 => 28,89 business days spent for managing or monitoring this asset. The maximum salary information is for business unit manager which is 7000TL and calculated using the exchange rate as 1,759, \$3979,53. System administrator’s monthly gross salary information was 3500TL which refers to \$1988,64 using exchange rate 1,759. This price is for a month and to calculate yearly gross amount => 1988,64 \* 12 = \$23863,68

As we calculated spent time for this asset was 28,89 days and then yearly salary for the workdays count calculated in *Chapter 4* on *page 65* as 261 days. The yearly gross amount salary is \$23863,68 then financial value of salary  $S(a)$  is;

$$S(a) = 23863,68 * 28,89 / 261$$

$$S(a) = \$2641,46$$

Yearly paid price  $Y(a)$  was calculated above and then financial value of asset  $F(t)$  is;  
For Windows Server 2003

$$F(t) = S(a) + Y(a)$$

$$F(t) = \$2641,46 + \$84,99$$

$$F(t) = \$2726,45$$

For Windows Server 2008

$$F(t) = S(a) + Y(a)$$

$$F(t) = \$2641,46 + \$80,99$$

$$F(t) = \$2722,45$$

Those financial values are for one package. When we look at assets list we cannot see the count of the asset, so that to apply our model to this asset, we have to find out the counts. When we look into assets list, we may found the count as;

- 2 DNS servers
- 1 mail server

- 1 SAN server
- 1 backup server
- 1 file server
- 1 data center server
- 2 virtual servers
- 26 servers in branches over the Turkey

Also this company has only Microsoft Operating Systems and all servers in branches are Windows Server 2003 and others are mentioned as new as Windows Server 2008. Now total count of Windows Server 2003 is 26 and count of Windows Server 2008 is 9.

Now we may calculate financial value using those counts as;

For Windows Server 2003

$$F(t) = \$2726,45 * 26 \Rightarrow F(t) = \$70887,7$$

For Windows Server 2008

$$F(t) = \$2722,45 * 9 \Rightarrow F(t) = \$24502,05$$

For the similar risks, we have to use total financial value which is the sum of those values and calculated as;

$$F(t) = \$70887,7 + F(t) = \$24502,05$$

$$F(t) = \$95389,75$$

Only the asset “Server Operating Systems” financial value is that. Now we may use this information for the total formula lets define what we have now;  $F(t)$  as \$95389,75 and  $R_{cur}(p, t)$  as 2 and then calculation is;

$$F_t(p) = R_{cur}(p, t) * F(t)$$

$$= 2 * \$95389,75$$

$$F_t(p) = 190779,5$$

This value refers to the yearly financial value of the vulnerability “Unauthorized person” and threat is “User error” over “Server Operating Systems” asset and this risks value defined at old list was  $I_a(p) = 8$  and also value of possibility and damage values are 1 and 3.

As mentioned the procedure of the organization [17], the result value of organization for this risk is  $1 * 3 * 8 \Rightarrow 24$  and it is under the acceptable limit for the company to make any workaround to reduce it.

Our model includes financial information and found the risk value as 190779,5. Also this value includes the financial value of the defined risk as \$95389,75. The decision to apply an action plan for this risk will be given by management. To help management, lets define minimum and maximum values for our model.

The importance value scale was mentioned above as  $125 \geq I_a(p) \geq 1$  and minimum value for average salary found for the organization is \$1988,64, maximum average salary information is . Also the scale for the current likelihood indicator was mentioned on page 80 as  $1 \geq P(t) \geq 0,12$  . Then let’s calculate minimum and maximum values;

$$\text{Minimum value: } 0,12 * 1 * \$1988,64 = > 238,64$$

$$\text{Maximum value: } 1 * 125 * \$3979,53 \Rightarrow 497441,25$$

So that the scale for  $F_t(p)$  is;

$$497441,25 \geq F_t(p) \geq 238,64$$

With the same thinking of acceptable level;

$$R_a = 238,64 + \frac{497441,25 - 238,64}{2}$$

$$R_a = 248839,95$$

Minimum and maximum values using values at organizations procedures are calculated below;

Maximum value of a risk =>  $1 * 1 * 1 * 1 * 1 * 1$  => 1

Maximum value of a risk =>  $5 * 5 * 5 * 5 * 5 * 5$  => 3125

Using the old matrix of implemented and defined solution in the organization's procedure, we may use to show risk score 91 different values. But with the new model we would have 146 different values to show the risk value. So the scale to show the risk value is expanded.

To evaluate financial values of threats and vulnerabilities for an asset easily, we developed software on ASP.NET framework, using SQL Server Database.

First we created the tables defined in Appendix A and created views and functions to calculate the financial value of asset as defined Chapter 3. You may see Appendix A to analyze the software.

## **CHAPTER 6**

### **CONCLUSION AND THE FUTURE WORK**

Organizations want to mitigate the risks to the acceptable level and first of all they have to see the risks and their financial values to define the risk mitigation plan and priorities. This is the main part of risk management process due to limited sources. Using this software we may manage our risk system easily. Also in new model within software we may have reports including financial values of the risk indicator and iteration of risk indicator in the whole score matrix. Using these reports, management may decide easily about which risks to be mitigated firstly and project plan and the order of risks to be mitigated. Also when deciding about this, they may see the financial value of the risk also.

At this model, we try to calculate every assets' financial value depending on threats and vulnerabilities individually. This model can be developed using process approach, thinking as a collection of assets, their vulnerabilities and threats together, to define more closer value of information security concepts. This type of calculation method may be more meaningful for IS Management to budget more effectively for risk mitigation.



## REFERENCES

- [1] A. Lenstra and T. Voss, "Information Security Risk Assessment , Aggregation , and Mitigation," pp. 391–401, 2004.
- [2] "FTS2001: Ready Reference Guide." [Online]. Available: <http://shop2.sprint.com/en/legal/fts2001/popup/popupFts2001ReadyReferenceGuide.shtml>. [Accessed: 07-Dec-2016].
- [3] W. Page, "ISO 27001 Security," *ISO 27000 Series*. [Online]. Available: <http://www.iso27001security.com>.
- [4] J. Roos, "Master Thesis on : Residual Risk Management," 2008.
- [5] Paul Hopkin, "Fundamentals of Risk Management > Part 3 > FIRM risk scorecard - Pg. 134e," *Fundamentals of Risk Management*, 2010. [Online]. Available: [http://my.safaribooksonline.com/book/-/9780749459420/14-risk-classification-systems/firm\\_risk\\_scorecard](http://my.safaribooksonline.com/book/-/9780749459420/14-risk-classification-systems/firm_risk_scorecard). [Accessed: 07-Dec-2016].
- [6] NIST, "NIST Special Publication 800-30 Revision 1," 2012.
- [7] M. S. Lund, B. Solhaug, and K. Stølen, *Model-Driven Risk Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.
- [8] Wiki, "ISO/IEC 27000 Series," *Wikipedia*. [Online]. Available: [http://en.wikipedia.org/wiki/ISO/IEC\\_27000-series](http://en.wikipedia.org/wiki/ISO/IEC_27000-series). [Accessed: 07-Dec-2016].
- [9] ISO, "ISO Web site." [Online]. Available: [www.iso.org](http://www.iso.org).
- [10] Joint Technical Committee ISO/IEC JTC 1, I. Technology, and I. S. techniques Subcommittee SC 27, "ISO/IEC 27005:2008." p. 61, 2008.
- [11] "ISO/IEC 27005 PDCA Model." [Online]. Available: [https://www.acisonline.net/images\\_article/image/ISO\\_IEC-27005\\_2008-and-COSO-ERM.jpg](https://www.acisonline.net/images_article/image/ISO_IEC-27005_2008-and-COSO-ERM.jpg). [Accessed: 07-Dec-2016].
- [12] Z. G. Ruthberg, W. T. Polk, N. I. of Standards, and T. (U.S.), *Report of the Invitational Workshop on Data Integrity*. U.S. Department of Commerce, National Institute of Standards and Technology, 1989.
- [13] S. Bosworth and M.E. Kabay, *Computer Security Handbook*. New York: John Wiley & Sons, Inc, 2002, p. 189.

- [14] H. F. Tipton, *Information Security Management Handbook*, no. v. 2. Auerbach, 2004.
- [15] The International Organization for Standardization and The International Electrotechnical Commission, “ISO/IEC 7498-2, open systems interconnection - security architecture. Technical report,” 1989.
- [16] Gelir İdaresi, “Gelir İdaresi Başkanlığı,” 2011. [Online]. Available: [http://www.gib.gov.tr/fileadmin/user\\_upload/Yararli\\_Bilgiler/amortisman\\_oranlari2011.html](http://www.gib.gov.tr/fileadmin/user_upload/Yararli_Bilgiler/amortisman_oranlari2011.html). [Accessed: 07-Dec-2016].
- [17] Ü. Şentürk, “Varlık ve Risk Yonetimi Proseduru.” Ankara, p. 7, 2010.
- [18] Pricegrabber, “Windows Server Prices,” *Web page*, 2013. [Online]. Available: <http://software.pricegrabber.com>. [Accessed: 07-Dec-2016].
- [19] ISO, “ISO/IEC 27009:2016,” *Web page*. [Online]. Available: [http://www.iso.org/iso/catalogue\\_detail?csnumber=42508](http://www.iso.org/iso/catalogue_detail?csnumber=42508). [Accessed: 07-Dec-2016].

## APPENDIX A

### RISK EVALUATION SOFTWARE

This software is developed using ASP.NET framework on MS SQL Server database.

Software has several sections like Constants, Controls, Inventories, Risks, Vulnerabilities, Threats, Analysis. Also at database part there tables, functions and views. You may see code and screenshots of software.

#### Table Definitions

Controls table includes applied control for the software. Recid column is an entity column and has auto incremental value. Every control has a number, name, description and a group. So we use this table to insert controls we will match the risks with the controls.

```
CREATE TABLE [dbo].[oss_controls](
    [recid] [int] IDENTITY(1,1) NOT NULL,
    [controlnum] [int] NULL,
    [controlname] [nvarchar](150) NULL,
    [controldesc] [nvarchar](250) NULL,
    [controlgroup] [nvarchar](50) NULL,
    CONSTRAINT [PK_oss_controls] PRIMARY KEY CLUSTERED
(
    [recid] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
```

Inventories table includes the assets and their information like price, ratios, scores, responsible, departments, average salary information of responsible, yearly price to pay as license or maintenance etc. Recid column is an entity column and has auto incremental value. Also creation date column has default value to get the system date automatically. Importance values which we will use in our model are stored at this table. Another value stores the count of days which is staff engagement with the related inventory.

```

CREATE TABLE [dbo].[oss_inventory](
    [recid] [int] IDENTITY(1,1) NOT NULL,
    [invname] [nvarchar](50) NOT NULL,
    [invdesc] [nvarchar](150) NULL,
    [invdept] [nvarchar](50) NULL,
    [invresp] [nvarchar](50) NULL,
    [passivedate] [date] NULL,
    [scoreconf] [numeric](8, 4) NULL,
    [scoreint] [numeric](8, 4) NULL,
    [scoreava] [numeric](8, 4) NULL,
    [invgroup] [nvarchar](50) NULL,
    [invgroup1] [nvarchar](50) NULL,
    [invlocation] [nvarchar](50) NULL,
    [credate] [datetime] NULL,
    [purchyear] [numeric](4, 0) NULL,
    [depratio] [numeric](8, 4) NULL,
    [maintenanceratio] [numeric](8, 4) NULL,
    [price] [numeric](10, 2) NULL,
    [yearlyprice] [numeric](10, 2) NULL,
    [avgsalaryofresp] [numeric](10, 2) NULL,
    [staffdaysinyear] [numeric](5, 2) NULL,
    CONSTRAINT [PK_oss_inventory] PRIMARY KEY CLUSTERED
    (
        [recid] ASC
    )

```

```
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
```

GO

```
ALTER TABLE [dbo].[oss_inventory] ADD CONSTRAINT
[DF_oss_inventory_ccreate] DEFAULT (getdate()) FOR [create]
GO
```

### Constants

Constants table is a generic table to have parameters for the software. Recid column is an entity column and has auto incremental value. Also there is a constraint for active to make default as “YES”.

```
CREATE TABLE [dbo].[oss_risk_constants](
    [recid] [int] IDENTITY(1,1) NOT NULL,
    [constname] [nvarchar](10) NULL,
    [constdesc] [nvarchar](50) NULL,
    [constval] [numeric](12, 4) NULL,
    [active] [nvarchar](10) NULL,
    CONSTRAINT [PK_oss_risk_constants1] PRIMARY KEY CLUSTERED
(
    [recid] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
```

GO

```
ALTER TABLE [dbo].[oss_risk_constants] ADD CONSTRAINT
[DF_oss_risk_constants1_active] DEFAULT (N'YES') FOR [active]
GO
```

Risks table is a collection of all risks which we use in the system. Recid column is an entity column and has auto incremental value. Also creation date column has default value to get the system date automatically.

```
CREATE TABLE [dbo].[oss_risks](
    [recid] [int] IDENTITY(1,1) NOT NULL,
    [riskname] [nvarchar](50) NULL,
    [riskdesc] [nvarchar](150) NULL,
    [credate] [datetime] NULL,
    [riskgroup] [nvarchar](50) NULL,
    CONSTRAINT [PK_oss_risks] PRIMARY KEY CLUSTERED
(
    [recid] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]

GO

ALTER TABLE [dbo].[oss_risks] ADD CONSTRAINT [DF_oss_risks_credate]
DEFAULT (getdate()) FOR [credate]

GO
```

Threats table is a collection of all threats which we use in the system. Recid column is an entity column and has auto incremental value. Also creation date column has default value to get the system date automatically.

```
CREATE TABLE [dbo].[oss_threats](
    [recid] [int] IDENTITY(1,1) NOT NULL,
    [threatname] [nvarchar](50) NULL,
    [threatdesc] [nvarchar](150) NULL,
    [threatgroup] [nvarchar](20) NULL,
    [create] [datetime] NULL,
    CONSTRAINT [PK_oss_threats] PRIMARY KEY CLUSTERED
(
    [recid] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]

GO

ALTER TABLE [dbo].[oss_threats] ADD CONSTRAINT [DF_oss_threats_create]
DEFAULT (getdate()) FOR [create]

GO
```

Vulnerability table is a collection of all vulnerabilities which we use in the system. Recid column is an entity column and has auto incremental value. Also creation date column has default value to get the system date automatically.

```
CREATE TABLE [dbo].[oss_vulnerability](
    [recid] [int] IDENTITY(1,1) NOT NULL,
    [vulnname] [nvarchar](50) NULL,
    [vulndesc] [nvarchar](150) NULL,
    [vulngroup] [nvarchar](20) NULL,
    [create] [datetime] NULL,
    CONSTRAINT [PK_oss_vulnerability] PRIMARY KEY CLUSTERED
(
    [recid] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]

GO

ALTER TABLE [dbo].[oss_vulnerability] ADD CONSTRAINT
[DF_oss_vulnerability_create] DEFAULT (getdate()) FOR [create]

GO
```



After defining all the values then we have to bring them together and match. We do this matching using Risk analysis table defined below. So matching, this table has crossreferences like foreign key constraint to other tables. Also this table includes the values for skill, access and source defined in Lenstra and Voss [1] Model. Also from traditions of the organization, we store possibility and damage scores. You may disable any risk matching using passive date.

```

CREATE TABLE [dbo].[oss_risk_analysis](
    [recid] [int] IDENTITY(1,1) NOT NULL,
    [invrecid] [int] NULL,
    [riskrecid] [int] NULL,
    [vulnrecid] [int] NULL,
    [threatrecid] [int] NULL,
    [controlrecid] [int] NULL,
    [description] [nvarchar](150) NULL,
    [create] [datetime] NULL,
    [skillscore] [decimal](8, 4) NULL,
    [access_score] [decimal](8, 4) NULL,
    [sourcedata] [decimal](8, 4) NULL,
    [pos_score] [decimal](8, 4) NULL,
    [damage_score] [decimal](8, 4) NULL,
    [passive_date] [date] NULL,
    CONSTRAINT [PK_oss_risk_analysis] PRIMARY KEY CLUSTERED
    (
        [recid] ASC
    )WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
    IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
    ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]

GO

ALTER TABLE [dbo].[oss_risk_analysis] WITH CHECK ADD CONSTRAINT
[FK_oss_risk_analysis_oss_controls] FOREIGN KEY([controlrecid])

```

```
REFERENCES [dbo].[oss_controls] ([recid])
```

```
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] CHECK CONSTRAINT  
[FK_oss_risk_analysis_oss_controls]
```

```
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] WITH CHECK ADD CONSTRAINT  
[FK_oss_risk_analysis_oss_inventory] FOREIGN KEY([invrecid])  
REFERENCES [dbo].[oss_inventory] ([recid])
```

```
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] CHECK CONSTRAINT  
[FK_oss_risk_analysis_oss_inventory]
```

```
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] WITH CHECK ADD CONSTRAINT  
[FK_oss_risk_analysis_oss_risks] FOREIGN KEY([riskrecid])  
REFERENCES [dbo].[oss_risks] ([recid])
```

```
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] CHECK CONSTRAINT  
[FK_oss_risk_analysis_oss_risks]
```

```
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] WITH CHECK ADD CONSTRAINT  
[FK_oss_risk_analysis_oss_threats] FOREIGN KEY([threatrecid])  
REFERENCES [dbo].[oss_threats] ([recid])
```

```
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] CHECK CONSTRAINT  
[FK_oss_risk_analysis_oss_threats]
```

```
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] WITH CHECK ADD CONSTRAINT
[FK_oss_risk_analysis_oss_vulnerability] FOREIGN KEY([vulnrecid])
REFERENCES [dbo].[oss_vulnerability] ([recid])
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] CHECK CONSTRAINT
[FK_oss_risk_analysis_oss_vulnerability]
GO
```

```
ALTER TABLE [dbo].[oss_risk_analysis] ADD CONSTRAINT
[DF_oss_risk_analysis_ccreate] DEFAULT (getdate()) FOR [create]
GO
```

### **Triggers**

Also to log the risk matching activities we created update and delete triggers to log the matching activities. Below you may see the source code of those triggers.

#### Update Trigger

```
USE [thesis]
GO
/***** Object: Trigger [dbo].[oss_risk_analysis_trg]    Script Date: 02/07/2013
23:07:59 *****/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
ALTER TRIGGER [dbo].[oss_risk_analysis_trg]
ON [dbo].[oss_risk_analysis]
for UPDATE
as
begin
declare @id int
select @id = recid from deleted
```

```
-- güncelleme için kayıt önce deleted (silinenler)
-- tablosuna gönderilir ardından da kayıt insert edilir
```

```
INSERT INTO oss_risk_analysis_log
    ([processdate]
    ,[recid]
    ,[invrecid]
    ,[riskrecid]
    ,[vulnrecid]
    ,[threatrecid]
    ,[controlrecid]
    ,[description]
    ,[create]
    ,[skillscore]
    ,[access_score]
    ,[sourcescore]
    ,[pos_score]
    ,[damage_score]
    ,[passive_date])
SELECT GETDATE() "processdate", recid, invrecid, riskrecid, vulnrecid, threatrecid,
controlrecid
, description, create, skillscore, access_score, sourcescore, pos_score,damage_score,
passive_date
FROM DELETED where recid=@id

end

Delete trigger;
USE [thesis]
GO
/***** Object: Trigger [dbo].[oss_risk_analysis_trg]    Script Date: 02/07/2013
23:07:59 *****/
SET ANSI_NULLS ON
GO
```

```

SET QUOTED_IDENTIFIER ON
GO
CREATE TRIGGER [dbo].[oss_risk_analysis_trg_del]
ON [dbo].[oss_risk_analysis]
for DELETE
as
begin
declare @id int
select @id = recid from deleted
-- güncelleme için kayıt önce deleted (silinenler)
-- tablosuna gönderilir ardından da kayıt insert edilir

INSERT INTO oss_risk_analysis_log
    ([processdate]
    ,[recid]
    ,[invrecid]
    ,[riskrecid]
    ,[vulnrecid]
    ,[threatrecid]
    ,[controlrecid]
    ,[description]
    ,[create]
    ,[skillscore]
    ,[access_score]
    ,[sourcescore]
    ,[pos_score]
    ,[damage_score]
    ,[passive_date])
SELECT GETDATE() "processdate", recid, invrecid, riskrecid, vulnrecid, threatrecid,
controlrecid
, description, create, skillscore, access_score, sourcescore, pos_score,damage_score,
passive_date
FROM DELETED where recid=@id

```

end

## Functions

To define daily financial value of asset , we are using calcDailyFinancialValue function defined below.

```
CREATE FUNCTION [dbo].[calcDailyFinancialValue]
(@recid int)
RETURNS numeric(10,2)
AS
BEGIN
declare @yearlyprice numeric(10,2)
declare @avgsalaryofresp numeric(8,4)
declare @workyear numeric(12,4)
declare @fval numeric(12,4)
declare @staffdays numeric(5,2)
declare @oran numeric(18,6)
declare @asgari numeric(5,2)
begin
        select      @workyear=constval      from      oss_risk_constants      where
constname='WORK-YEAR'
end
begin
        select @asgari=constval from oss_risk_constants where constname='WAGE-
MINI'
end
select @yearlyprice = yearlyprice,
@avgsalaryofresp = isnull(avgsalaryofresp,isnull(@asgari,550)),
@staffdays = isnull(staffdaysinyear,1)
from oss_inventory
where recid=@recid

set @oran = @avgsalaryofresp*12 / @workyear
```

```

set @fval = (@yearlyprice/@workyear) + @oran
--begin
--update oss_inventory set yearlyprice=@yearlyprice
--      where recid=@recid
--end
return @fval

end

```

Also yearly financial value of asset is calculated with the function named as calcYearlyFinancialValue defined below.

```

CREATE FUNCTION [dbo].[calcYearlyFinancialValue]
(@recid int)
RETURNS numeric(10,2)
AS
BEGIN
declare @yearlyprice numeric(10,2)
declare @avgsalaryofresp numeric(8,4)
declare @workyear numeric(12,4)
declare @fval numeric(12,4)
declare @staffdays numeric(5,2)
declare @oran numeric(18,6)
declare @asgari numeric(5,2)

begin
select @workyear=constval from oss_risk_constants where constname='WORK-
YEAR'
end
begin
select @asgari=constval from oss_risk_constants where constname='WAGE-
MINI'
end

```

```

select @yearlyprice = yearlyprice,
@avgsalaryofresp = isnull(avgsalaryofresp,isnull(@asgari,550)),
@staffdays = isnull(staffdaysinyear,1)
from oss_inventory
where recid=@recid

set @oran = @avgsalaryofresp*12*@staffdays / @workyear
set @fval = @oran + @yearlyprice

```

```

--begin
--update oss_inventory set yearlyprice=@yearlyprice
--      where recid=@recid
--end
return @fval

end

```

To analyze the results we use a view. With this view, we may see all information about asset, risk, vulnerability and threat. Also we may see the financial values of the inventories and their current likelihood indicators.

## Views

```

CREATE VIEW [dbo].[oss_risk_analyze]
AS
SELECT          ora.recid,  oc.controlnum,  oc.controlname,  oc.controldesc,
oc.controlgroup,  oi.invname,  oi.invdesc,  oi.invdept,  oi.invresp,  oi.scoreconf,
oi.scoreint, oi.scoreava,
                oi.invlocation,  orr.riskname,  orr.riskdesc,  orr.riskgroup,  ot.threatname,
ot.threatdesc,  ot.threatgroup,  ov.vulnname,  ov.vulndesc,  ov.vulngroup,
ora.access_score,
                ora.skillscore,  ora.sourcescore,  ora.damage_score,  ora.description,
ora.credate,  ora.pos_score,  oi.price,  CAST(ISNULL(oi.yearlyprice,
dbo.calcYearPrice(oi.recid))

```



```

AS numeric(18, 2)) AS yearprice,
CAST(dbo.calcYearlyFinancialValue(oi.recid) AS numeric(18, 2)) AS financialval,
CAST(dbo.calcDailyFinancialValue(oi.recid)
AS numeric(18, 2)) AS dailyfinancialval, CAST(oi.scoreconf *
oi.scoreint * oi.scoreava * ora.access_score * ora.skillscore * ora.sourcescore AS
numeric(8, 4))
AS CurrentRiskIndicator, osi.iteracount AS iteration,
CAST(osi.iteracount / 2000 AS numeric(5, 2)) AS iterange
FROM dbo.oss_risk_analysis AS ora INNER JOIN
dbo.oss_controls AS oc ON ora.controlrecid = oc.recid INNER JOIN
dbo.oss_inventory AS oi ON ora.invrecid = oi.recid INNER JOIN
dbo.oss_risks AS orr ON ora.riskrecid = orr.recid INNER JOIN
dbo.oss_threats AS ot ON ora.threatrecid = ot.recid INNER JOIN
dbo.oss_vulnerability AS ov ON ora.vulnrecid = ov.recid LEFT OUTER
JOIN
dbo.oss_score_iteration AS osi ON ROUND(oi.scoreconf * oi.scoreint
* oi.scoreava * ora.access_score * ora.skillscore * ora.sourcescore, 8, 4) = osi.score
WHERE (oi.passivedate IS NULL) AND (ora.passive_date IS NULL)

```

## Software screenshots

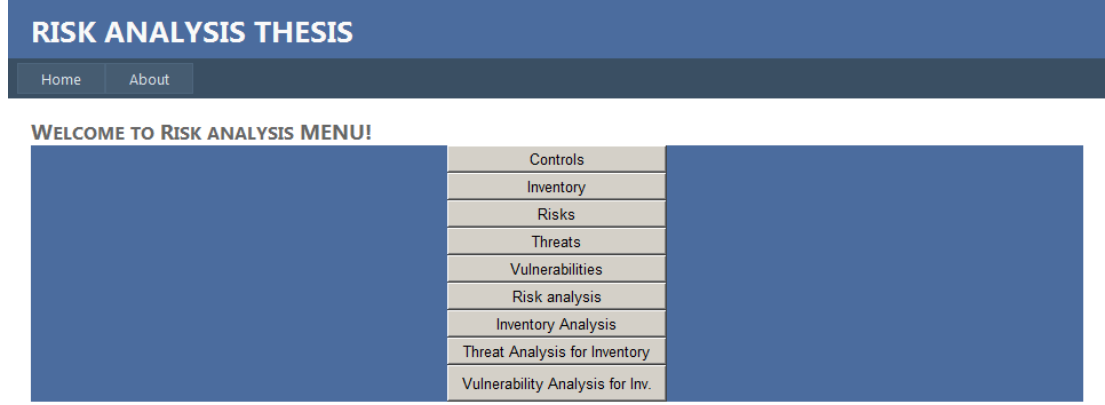


Figure A.1 Software-menu screenshot

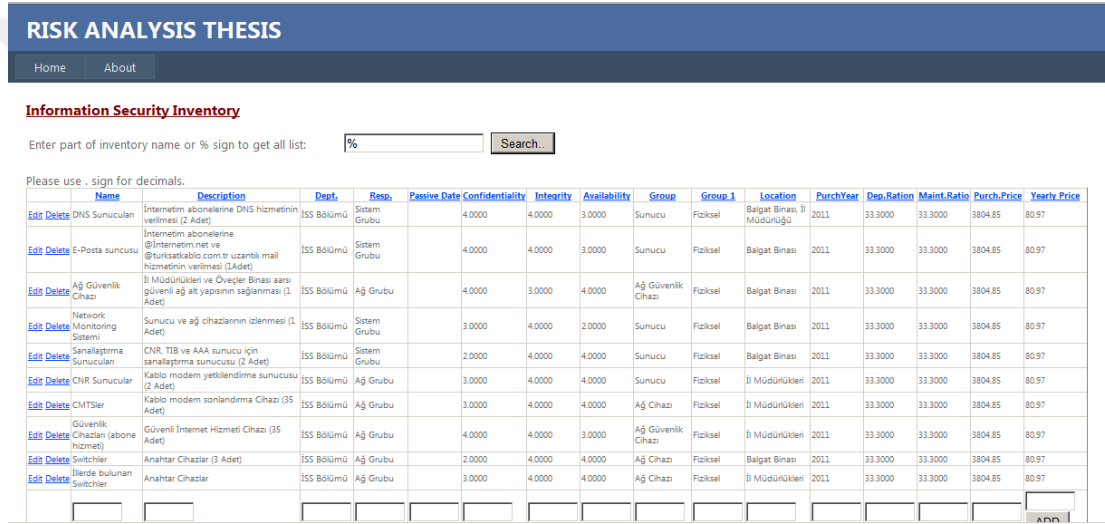


Figure A.2 Software-Inventory definition screenshot

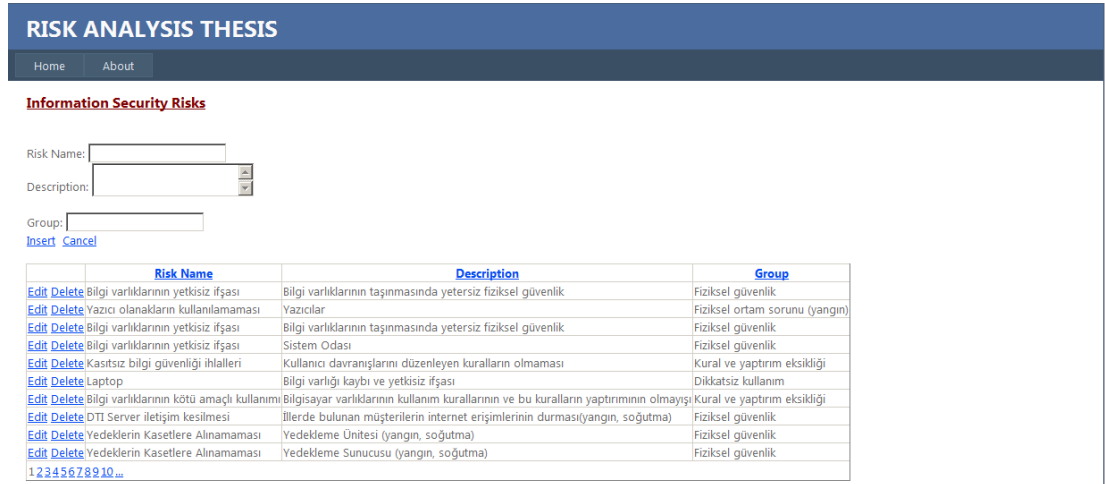


Figure A.3 Software-risk definition screenshot

# RISK ANALYSIS THESIS

[Home](#)[About](#)

## Information Security Controls

Control No:

Name :

Description:

Control Group:

[Insert](#) [Cancel](#)

	<a href="#">Control No</a>	<a href="#">Control Name</a>	<a href="#">Control Desc</a>	<a href="#">Control Group</a>
<a href="#">Edit</a> <a href="#">Delete</a>	1	GENERAL	GENERAL	POLICY

Figure A.4 Software-Control definition screenshot

# RISK ANALYSIS THESIS

[Home](#)[About](#)

## Information Security Threats

Threat Name:

Description:

Group:

[Insert](#)

	<a href="#">Name</a>	<a href="#">Description</a>	<a href="#">Group</a>	<a href="#">Creation Date</a>
<a href="#">Edit</a> <a href="#">Delete</a>	Ağ yöneticisinin görevde olmaması	Ağ Yöneticisi-Ağ yönetiminin sağlıklı gerçekleştirilememesi	Personel	
<a href="#">Edit</a> <a href="#">Delete</a>	Alınması gereken kararların zamanında alınmaması	Direktör-Yönetimsel işlemlerde gecikme ve durma	Personel	
<a href="#">Edit</a> <a href="#">Delete</a>	Aşırı iş yüklenmesi	Kaynak yönetimi	Personel	
<a href="#">Edit</a> <a href="#">Delete</a>	BGYS sorumlusunun görevde olmaması	BGYS Sorumlusu-BGYS işlemlerinin aksaması	Personel	
<a href="#">Edit</a> <a href="#">Delete</a>	Bilgi güvenliği ihlalleri	-	İhlal yönetimi	
<a href="#">Edit</a> <a href="#">Delete</a>	Bilgi işlem kaynaklarının hasar görmesi	Yangından Korunma Hizmetinin Alınması-Bilgi işlem faaliyetlerinin aksaması	Hizmet yönetimi	
<a href="#">Edit</a> <a href="#">Delete</a>	Bilgi varlıkları ile ilgili bilgi sızdırılması	Sistem Odası-Bilgi varlıklarının yetkisiz ifşası	Fiziksel güvenlik	
<a href="#">Edit</a> <a href="#">Delete</a>	Bilgi varlıklarının kötü amaçlı kullanımı	-Bilgi varlıklarının yetkisiz ifşası	Disiplin	
<a href="#">Edit</a> <a href="#">Delete</a>	Bilgi varlıklarının yetkisiz kullanımı	Temizlik Hizmetinin Alınması-Bilgi varlıklarının yetkisiz kullanımı sebebiyle varlıkların kullanılamaz duruma gelmesi	Hizmet	

Figure A.5 Software-Threat definition screenshot

## RISK ANALYSIS THESIS

Home About

### Information Security Vulnerabilities

Name

Description

Group

[Insert](#)

	Name	Description	Group	Creation Date
<a href="#">Edit</a> <a href="#">Delete</a>	Ağ erişim sorunu		Ağ erişim sorunu	
<a href="#">Edit</a> <a href="#">Delete</a>	Ağ Güvenlik Cihazı	Hizmetin durması	Fiziksel güvenlik	
<a href="#">Edit</a> <a href="#">Delete</a>	Arıza Kayıt Formları	Arıza kayıtlarına ulaşılamaması	Fiziksel güvenlik	
<a href="#">Edit</a> <a href="#">Delete</a>	Bilgi Güvenliği Yönetim Sistemi Dokümanları	Kötü niyetli kişilerin eline geçmesi dolayısıyla sabotaj	Yetkisiz erişim	
<a href="#">Edit</a> <a href="#">Delete</a>	Bilgi İşlem Varlıkları İçin Teknik Destek Alınması	Bilgi işlem faaliyetlerinin aksaması	Ağ erişim sorunları	
<a href="#">Edit</a> <a href="#">Delete</a>	Bilgi varlıklarının imhası	Bilgi varlıklarının imhasında bilgi güvenliğin ihlali	İmha	
<a href="#">Edit</a> <a href="#">Delete</a>	Yetersiz fiziksel güvenlik	Bilgi varlıklarının yetkisiz ifşası	Fiziksel güvenlik	
<a href="#">Edit</a> <a href="#">Delete</a>	CMTS ler erişime açık	Müşterilerin internet erişimlerinin durması	Fiziksel güvenlik	
<a href="#">Edit</a> <a href="#">Delete</a>	CNR Sunucular	Müşteri modellerinin yeklendirilmesinin gerçekleştirilememesi	Fiziksel güvenlik	
<a href="#">Edit</a> <a href="#">Delete</a>	DNS Servisi		Ağ erişim sorunu	

1 2 3 4 5 6

Figure A.6 Software-Vulnerability definition screenshot

http://localhost:1036/RiskAnalysis.aspx

## RISK ANALYSIS THESIS

Home About

### Risk Matching

Inventory  Risk

Vulnerability  Threat

Control

Description of Risk

Skill

Access from

Source of threat

Optional Possibility

Damage

Passive date

[Insert](#)

Control No	Control Name	Inventory	Inv.Descr.	Responsible	Confid.Score	Intes.Score	Avail.Score	Location	Risk name	Threat name	Vuln.name	Access Score	Skill Score	Source Score	Damage Score	Possib.Score	Description
1	GENERAL	DNS Sunucular	İnternetin abonelerine DNS hizmetinin verilmesi (2 Adet)	Sistem Grubu	4.0000	4.0000	3.0000	Balgat Binası, II Müdürlüğü	Hizmetin durması	Saldırı	Güncel olmayan sürümler	1.0000	0.9000	1.0000			
1	GENERAL	DNS Sunucular	İnternetin abonelerine DNS hizmetinin verilmesi (2 Adet)	Sistem Grubu	4.0000	4.0000	3.0000	Balgat Binası, II Müdürlüğü	Bilgi varlıklarının yetkisiz ifşası	Güvenlik lehtian	Güncel olmayan sürümler	1.0000	0.9000	1.0000			

Figure A.7 Software-Risk matching

## RISK ANALYSIS THESIS

Home About

Enter part or full of inventory name

Inventory Name	Description	Department	Responsible	Location	Control	Name	Description	Group	Risk	Description	Group	Vulnerability	Description	Group	Threat	Description	Group	Confidentiality	Integrity	Availability	Accessibility	Skill	Source	Damage	Possibility
DNS Sunucular	İnternetin abonelerine DNS hizmetinin verilmesi (2 Adet)	ISS B60Ümü	Sistem Grubu	Balgat Binası, II Müdürlüğü	1	GENERAL	GENERAL	POLICY	Hizmetin durması	Ağ Güvenlik Cihazı (yapılandırma)	Fiziksel güvenlik	Güncel olmayan sürümler	Yazılımlarda güncelleme problemi	Güncelleme	Saldırı	Hizmetin durması	Güvenlik yönetimi	4.0000	4.0000	3.0000	1.0000	0.9000	1.0000		
DNS Sunucular	İnternetin abonelerine DNS hizmetinin verilmesi (2 Adet)	ISS B60Ümü	Sistem Grubu	Balgat Binası, II Müdürlüğü	1	GENERAL	GENERAL	POLICY	Bilgi varlıklarının yetkisiz ifşası	Bilgi varlıklarının taşınmasında yetersiz fiziksel güvenlik	Fiziksel güvenlik	Güncel olmayan sürümler	Yazılımlarda güncelleme problemi	Güncelleme	Güvenlik açıkları	Yama Raporlarına Hizmetinin Alınmaması	Güncelleme/erişim zamanında yapılamaması	4.0000	4.0000	3.0000	1.0000	0.9000	1.0000		

Figure A.8 Software-Inventory Analysis

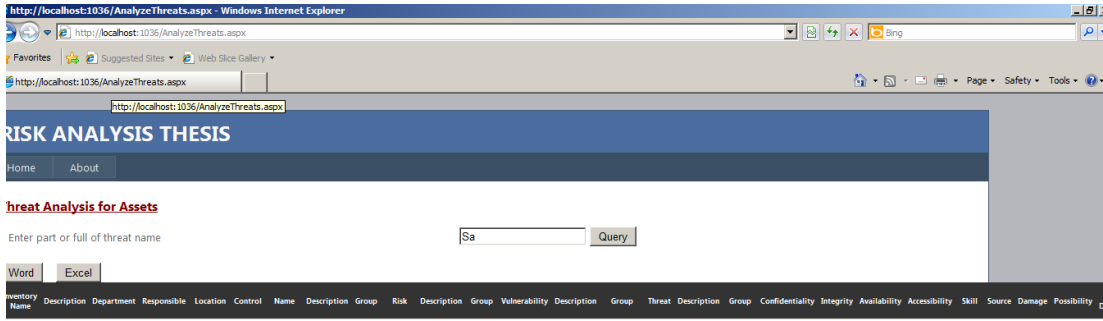


Figure A.9 Software-Threat analysis screenshot

Damage	Possibility	Risk Description	Purch Price	Yearly price	Yearly Financial Val	Creation Date
			5000.00	1665.00	25528.68	2/7/2013 2:53:38 PM

Figure A.10 Software-Threat analysis screenshot 2

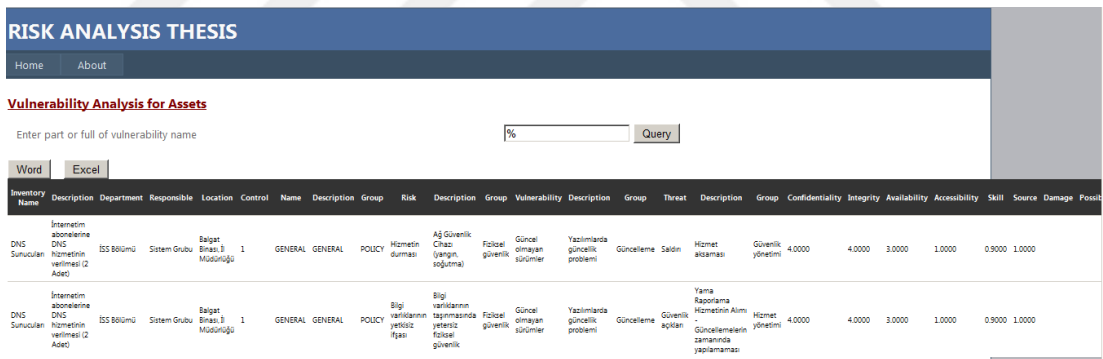


Figure A.11 Software-Vulnerability analysis screenshot

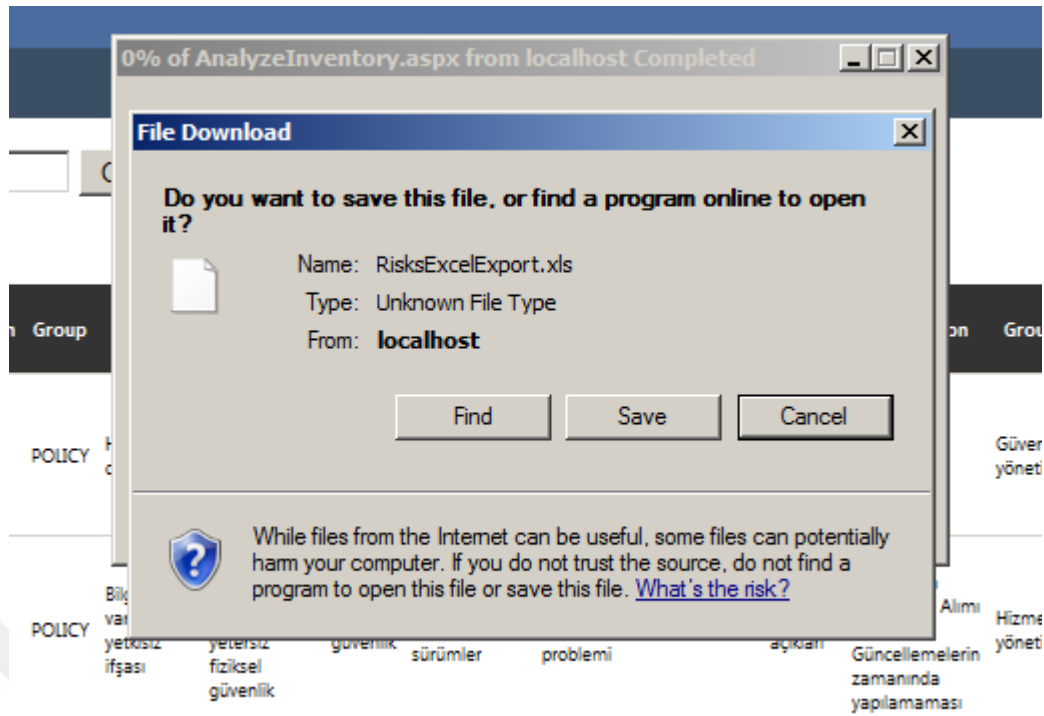


Figure A.12 Software-MS Excel Export

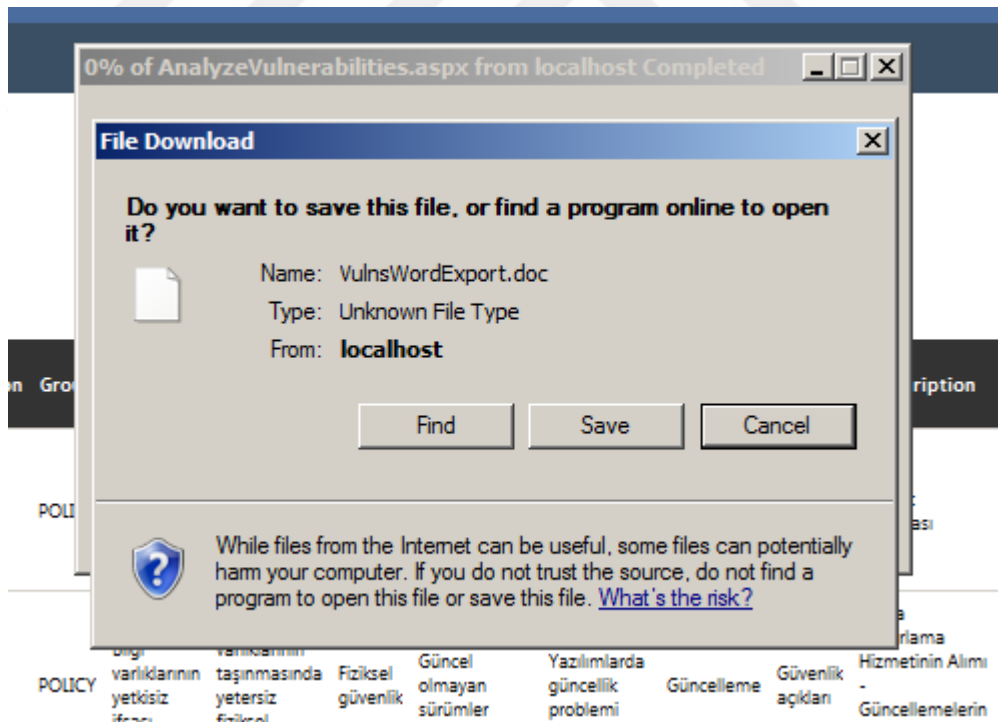


Figure A.13 Software-MS Word Export

## APPENDIX B

### CURRICULUM VITAE

#### PERSONAL INFORMATION

Surname, Name: Şereflisan, Oğuzhan  
Nationality: Turkish (TC)  
Date and Place of Birth: 02 July 1976 , Artvin  
Marital Status: Married  
Phone: +90 312 433 33 69  
Email: oguzhan.sereflisan@gmail.com

#### EDUCATION

Degree	Institution	Year of Graduation
BS	Erciyes University Control and Computer Engineering	2001
High School	STFA Anatolian Technical High School	1994

## WORK EXPERIENCE

2013-Present	HAVELSAN A.Ş.	R&D Engineer, Project Manager
2012-2013	Pozitif Değer Mühendislik ve Danışmanlık Ltd. Şti	IS Consultant
2011-2012	Genpower	IS Manager
2009-2011	Türksat	Senior Specialist
2003-2009	Türk Traktör	Specialist
1999-2001	Şahin Yazılım	Analyst Programmer

## FOREIGN LANGUAGES

Very Good English, Beginner Russian

## PROFESSIONAL AFFILIATIONS

Turkish Informatics Association, Trabzonspor Congress Membership, Association of Computer Engineers