AN AUTOMATED TOOL FOR INFORMATION SECURITY MANAGEMENT SYSTEM

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

AHMET ERKAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

SEPTEMBER 2006

Approval of the Graduate School of Informatics

_____

Assoc. Prof. Nazife BAYKAL

Director

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

_____

Assoc. Prof. Yasemin YARDIMCI

Head of Department

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

_____

Dr. Ali ARİFOĞLU

Supervisor

Examining Committee Members

Prof.Dr. Semih BİLGEN	(METU, EE)	_____
Dr.Ali ARİFOĞLU	(METU, IS)	_____
Assoc.Prof.Dr.Ali DOĞRU	(METU, CENG)	_____
Dr.Sevgi ÖZKAN	(METU, IS)	_____
Prof.Dr.Ali YAZICI	(TOBB-ETU, CENG)	_____

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. All comments in this thesis reflect my personal opinions and cannot be regarded as the opinions of Turkish Armed Forces.

Name, Surname: Ahmet ERKAN

Signature : _____

ABSTRACT

AN AUTOMATED TOOL FOR INFORMATION SECURITY MANAGEMENT SYSTEM

ERKAN, Ahmet
M.S., Department of Information Systems
Supervisor: Dr. Ali ARİFOĞLU

September 2006, 94 pages

This thesis focuses on automation of processes of Information Security Management System. In accordance with two International Standards, ISO/IEC 27001:2005 and ISO/IEC 17799:2005, to automate the activities required for a documented ISMS as much as possible helps organizations. Some of the well known tools in this scope are analyzed and a comparative study on them including "InfoSec Toolkit", which is developed for this purpose in the thesis scope, is given. "InfoSec Toolkit" is based on ISO/IEC 27001:2005 and ISO 17799:2005. Five basic integrated modules constituting the "InfoSec Toolkit" are "Gap Analysis Module", "Risk Module", "Policy Management Module", "Monitoring Module" and "Query and Reporting Module". In addition a research framework is proposed in order to assess the public and private organizations' information security situation in Turkey.
Keywords: Information security, information security management system, ISMS, ISO/IEC 27001:2005, ISO/IEC 17799:2005.

ÖZ

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ İÇİN OTOMATİK BİR ARAÇ

ERKAN, Ahmet
Yüksek Lisans, Bilişim Sistemleri Bölümü
Tez Yöneticisi: Dr. Ali ARİFOĞLU

Eylül 2006, 94 sayfa

Bu tez Bilgi Güvenliği Yönetim Sistemi süreçlerinin otomasyonunu konu alır. ISO/IEC 27001:2005 ve ISO/IEC 17799:2005 standartlarına uygun olarak dokümante edilmiş bir BGYS için gerekli faaliyetlerin mümkün olduğunca otomatikleştirilmesi kurumlara yardım olacaktır. Bu amaçla "InfoSec Toolkit" adında bir araç geliştirilmiştir. Bu tezde, bu alandaki çok bilinen araçlar ve bunlara ilave olarak bu amaç için üretilmiş olan "InfoSec Toolkit" ile ilgili karşılaştırmalı bir çalışma sunulmaktadır. "InfoSec Toolkit" ISO/IEC 27001:2005 ve ISO 17799:2005 standartlarına dayanılarak hazırlanmıştır. "InfoSec Toolkit" i oluşturan birbiriyle entegre beş temel modül şunlardır; "Gap Analysis Module", "Risk Module", "Policy Management Module", "Monitoring Module" ve "Query and Reporting Module". Ayrıca, Türkiye'deki kamu ve özel kurum/kuruluşların bilgi güvenliği hususundaki mevcut durumlarını belirmek için bir araştırma çerçevesi önerilmektedir.

Anahtar Kelimeler: Bilgi güvenliği, bilgi güvenliği yönetim sistemi, BGYS, ISO/IEC 27001:2005, ISO/IEC 17799:2005.

To my wife Nefiye.

ACKNOWLEDGEMENTS

I first thank my supervisor Dr. Ali ARİFOĞLU for providing guidance and insight throughout this research.

I also want to thank my colleague Ahmet Şakir GENÇ for joint studies and his suggestions and recommendations. And I want to thank my friend Edem ÖNK for his aids and suggestions.

Finally, I offer sincere thanks to my wife Nefiye for her great faith in me and her patience to endure me during this period.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

AS/NZS	:	Australia Standards/New Zealand Standards
A.Ş.	:	Anonim Şirket
BGYS	:	Bilgi Güvenliği Yönetim Sistemi
BS	:	British Standard
BSI	:	British Standard Institute
COBIT	:	The Control Objectives for Information and Related Technology
COBRA	:	Consultative, Objective and Bi-functional Risk Analysis
CSI/FBI	:	Computer Security Institute/Federal Bureau of Investigation
DISC	:	Delivering Information Solutions to Customers
DoS	:	Denial of Service
DPT	:	Devlet Planlama Teşkilatı
EAR	:	Environment for the Analysis of Risk
IIS	:	Internet Information Service
InfoSec	:	Information Security
ISMS	:	Information Security Management System
ISO	:	The International Standards Organization
IEC	:	The International Electrotechnical Commission
IT	:	Information Technology
JTC	:	The Joint Technical Committee
METU	:	Middle East Technical University
MSAT	:	Microsoft Security Assessment Tool
NIST	:	National Institute of Standards and Technology
NIST SP	:	National Institute of Standards and Technology Special Publication

OECD	:	The Organization for Economic Cooperation and Development
PDCA	:	Plan-Do- Check-Act
PDF	:	Portable Document Format
SOA	:	Statement of Applicability
TR	:	Technical Report
TSE	:	Türk Standartları Enstitüsü
UK	:	United Kingdom
UML	:	Unified Modelling Language

LIST OF STANDARDS

- ISO/IEC 17799:2005(E), Information technology — Security techniques — Code of practice for information security management.
- ISO/IEC 27001:2005(E), Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management
- ISO/IEC TR 13335-3:1998(E), Information technology — Guidelines for the management of IT Security — Techniques for the management of IT Security
- Guide to BS 7799 Risk Assessment (PD 3002) – Guidance aimed to those responsible for carrying out risk management.
- "Are you ready for a BS 7799 Audit? (DISC PD 3003) – A compliance assessment workbook".
- NIST SP 800-53, Revision 1, "Recommended Security Controls for Federal Information Systems," 2006.

CHAPTER 1

INTRODUCTION

1.1 Background

Information is a critical resource for all organizations since information supports business continuity and commerce and helps managers and staff to make appropriate and effective decisions. Securing organizational information and its critical elements, including the systems and hardware that use, store, and transmit that information have become more and more important.

According to the ISO/IEC 17799:2005, information is an important asset as other important business assets for every organization. It is crucial to an organization's business and thus shall be protected properly. Information security can described as to protect information from various threats to ensure business continuity, minimize risks and maximize profits and business opportunities [1].

If the organization can not secure its information, severe impact on business continuity and business credibility can occur. If the organization's information assets are lost, pass into the wrong hands or in any wise are misused, it can be

catastrophic to the organization, and equally catastrophic to other parties doing business, directly or indirectly, with this organization.

There is a need to be assured that the organizations have adequate routines and procedures so that organizations are able to trust each other concerning the handling of critical information and shareholders are able to trust the organizations' ability to do so. In order to respond to this need and to ensure organizations to protect their information assets (not only the IT-related information assets), two interlinked international standards, ISO/IEC 17799:2005 and ISO/IEC 27001:2005, were prepared by Joint Technical Committee ISO/IEC JTC 1. The first one can be described as a set of best practices for dealing with information security and the latter provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) [2].

A descriptive is figure given in Figure 1 [3]. Figure 1 shows the relations between threats, threats agents, assets and vulnerabilities and safeguards as seen from the ISO/IEC 17799:2005 [1].

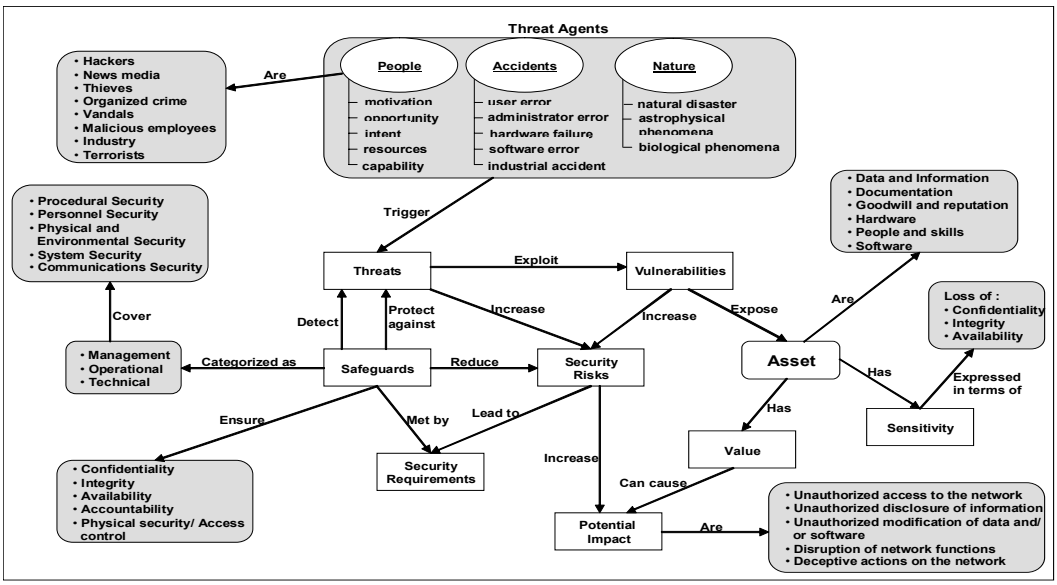


Figure 1– Relationship between asset, threat, vulnerability and safeguards [3].

Since ISO/IEC 17799:2005 is flexible and neutral enough to be used in any organization, it is easy for users to have difficulties during adoption. Without having a pre-understanding of information security and understanding how these standards work, trying to adopt these standards will be of no real value to the organizations adopting these standards. If the organizations do not have adequate knowledge about mentioned issues they might end up with a false sense of security.

Organizations need to address potential incidents that can harm their information assets, and produce a roadmap of what is to be done to protect information assets. The most optimal way to deal with risks is to apply a structured method of working towards risk handling and security. This is often done through risk analysis/assessment, where the risks are highlighted and plans on how to mitigate, avoid, or otherwise treat them are produced. Conducting a risk assessment is considered to be of such great importance that it is stated as one of the key requirements in the ISO/IEC 27001:2005.

ISO/IEC 27001:2005 is a model prepared for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) [2]. For organizations to protect information assets and give confidence to interested parties one of the best ways is to adopt an ISMS.

1.2 Problem

Most of the organizations find it difficult and costly to deal with the Information Security in a proper way. When a new vulnerability or a new virus is detected or launched, the consequences can be comprehensive on the fly. In addition, it is clear that interoperability between organizations is important and will become more important in the future. To provide fast and appropriate response to security incidents and to ensure interoperability between organizations, there is a need for a systematic and pre-defined approach to deal with Information Security challenge.

Thus, how to handle the Information Security challenge will then be of importance. One of the best ways of handling Information Security challenge is to adopt ISO/IEC 27001:2005.

To adopt ISO/IEC 27001:2005 is a complicated process and needs so much time. To reduce adoption time in a reasonable degree is another problem for the organizations who decide to adopt this standard.

1.3 Objective

The objectives of this thesis are given below

- To offer a toolkit to organizations for their ISO/IEC 27001:2005 adoption process to automate activities required for a documented ISMS as much as possible. Our toolkit's name is "InfoSec Toolkit". "InfoSec Toolkit" is based on TS ISO/IEC 27001. It has four basic integrated modules which are "Gap Analysis Tool", "Risk Management Tool", "Policy Management Tool" and "Monitoring Tool".
- Using "Gap Analysis Tool" which is one of the sub modules of "InfoSec Toolkit" a framework is given. This framework is aimed to show current situation of the organizations about Information Security.
- Since at present there is only one tool prepared in Turkish and it is limited, the aim of this thesis is to produce a Turkish tool for this purpose. This toolkit can be prepared in some other languages as future work.

1.4 Thesis Structure

This text is organized as follows:

Chapter 2 provides the related research on Information Security. Firstly, in this section subsequently, some basic concepts about Information Security will be given. Next, an explanation of what ISO/IEC 17799:2005 and ISO/IEC 27001:2005 are and how they are used will be given, subsequently. And lastly a

study is given which analyzes some of the well known tools, a comparative study on them and the “InfoSec Toolkit”.

Chapter 3 includes the approach adopted by this thesis “Infosec Toolkit” that covers initial gap analysis, risk management, policy management, monitoring and querying and reporting on information generated these processes in detail. In addition it covers a research framework used for evaluating organizations’ current situation of information security.

Chapter 4 explains implementation details of this approach.

Chapter 5 covers the justification of the implemented system, “Infosec Toolkit”.

Chapter 6 provides the conclusions, possible future work directions for the subsystems and function of the study in means of contribution effort in the “InfoSec Toolkit” project.

CHAPTER 2

RELATED RESEARCH

This chapter introduces main issues about Information Security, and the two interlinked ISO standards, ISO/IEC 17799:2005 and ISO/IEC 27001:2005. Also compression of tools developed by now in order to help organizations during the creating a documented ISMS process.

2.1 Information Security

As mentioned in Chapter one, one of the most critical assets for any organization is information. It increases the value of the organization that is why I must be protected properly. Nowadays most of the organizations do business with other organizations. As a result of this, the need for interconnected business environment is increasing constantly. And this situation makes information vulnerable because of a number and a wider variety of threats and vulnerabilities.

Information can be in different forms. It can be written or printed on paper. It can be stored electronically, transmitted by electronic means or by post. It can be

spoken in conversation or shown on videos. No matter what form information takes or in what way it is stored or shared, it should always be properly protected [1].

It is a common misunderstanding that information security deals specifically with computer security. But in fact it deals with the need and desire to protect information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Through the years computer security has focused on several issues. In the beginning, it focused mostly on technical issues such as encryption, access controls and intrusion detection systems. According to the results of CSI/FBI Computer Crime and Security Survey – 2005 economic, financial and risk management aspects of computer security have also become important concerns to the organizations. These concerns are complements to the technical aspects of computer security [4].

Information security is, according to the internationally recognized code of information security best practice, ISO/IEC 17799: 2005, the 'preservation of the confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved' [1].

- Confidentiality[1]. ISO has defined confidentiality as "the property that information is not made available or disclosed to unauthorized individuals, entities, or processes" [2]. If data is not handled adequately to safeguard the confidentiality of related information. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc.

[1] RUSecure Information Security Glossary, Retrieved August 22, 2006, from http://www.yourwindow.to/information-security/gl_confidentialityintegrityandavailabili.htm

- Integrity. ISO has defined integrity as “the property of safeguarding the accuracy and completeness of assets” [2]. The integrity of data is not only whether the data is “correct”, but whether it can be trusted and relied upon. For example, making copies (say by e-mailing a file) of a sensitive document, threatens both confidentiality and the integrity of the information. Because, by making one or more copies, the data is then at risk of change or modification.
- Availability. ISO has defined availability as “the property of being accessible and usable upon demand by an authorized entity” [2]. Availability can be ensured by for example, in a business context having the web portal secured against Denial of Service (DoS) attacks or ensuring that the computer infrastructure is redundant enough to allow people to do their job during incidents. If availability can not be ensured in an organization’s systems, this might result in processes or people not being able to perform their tasks in due time.

2.2 Risk Assessment

ISO/IEC 17799: 2005 is about management of risk, which is accomplished by developing a risk management and mitigation strategy, whereby assets, threats, and vulnerabilities are identified and the commensurate risk is quantified.

Risk management is a systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risk.

Risk assessment is an important part of risk management and deals with identifying and grading risks to the organization. Risk assessment consists of risk analysis and risk evaluation. Risk analysis is the systematic approach of estimating the magnitude of risks. Risk evaluation is and the process of comparing the estimated risks against risk criteria to determine the significance of the risks [1]. Risk assessment should fulfill all criteria listed below:

- Identifying all assets
- Identifying threats and vulnerabilities, and any other applicable security requirements
- Identifying the impacts that loses of confidentiality, integrity and availability might have on the assets
- Based on this information, assessing the harm and likelihood of risks occurring, and estimating the levels of risk
- Identifying the most appropriate risk treatment option
- Select control objectives to reduce the risks to an acceptable level [5].

The deliverable produced by these steps needs to be up to date and hence should be revised on a regular basis.

There are many different methodologies for assessing risks, but most are based on one of two approaches: quantitative risk management or qualitative risk management.

Quantitative risk assessment: Quantitative risk assessment describes risks from a purely mathematical viewpoint, fixing a numerical value to every risk and using that as a guideline for further risk management decisions [6]. For instance, the true value of each business asset is estimated in terms of what it would cost to replace it, what it would cost in terms of lost productivity, what it would cost in terms of brand reputation, and other direct and indirect business values. The same objectivity is used when computing asset exposure, cost of controls, and all of the other values identified during the risk management process.

While using this method, risk is often described by a mathematical formula:

$$Risk = Threat * Vulnerability * Asset\ Value \qquad \text{(Equation 1)}$$

For example; the threat is that web server of the organization being hacked and likelihood to that threat is assigned. In this case, say that it is 80 percent likely that a hacker will hack the web server of the organization unless something else intervenes (a countermeasure). The vulnerability is the web server's weakness. The fact that the web server is unable to defend itself adequately against this hacking attack means that the server is probably 100 percent likely to be harmed by a successful attack of a hacker. And the value of the asset is calculated. The cost of disclosure of the information on the web server or unavailability of the web server or something else is $1000.

Therefore, the total risk in this scenario is:

Risk = 80% * 100% * $1000.00.
Risk = $800.00

The other risk analysis method is qualitative risk analysis. The qualitative methodology attempts only to prioritize the various risk elements in subjective terms [7].

Qualitative risk assessment: In this method it is not needed to assign hard financial values to assets, expected losses, and cost of controls. Instead, relative values are calculated. Risk analysis is usually conducted through a combination of questionnaires and collaborative workshops involving people from a variety of groups within the organization such as information security experts; information technology managers and staff; business asset owners and users; and senior managers.

The benefits of a qualitative approach are that it overcomes the challenge of calculating accurate figures for asset value, cost of control, and so on, and the process is much less demanding on staff. Qualitative risk management projects can typically start to show significant results within a few weeks, whereas most

organizations that choose a quantitative approach see little benefit for months, and sometimes even years, of effort. Although there are many well-developed industries that use quantitative risk, it is not commonly used in information technology[2].

2.3 Background to ISO Information Security Management System Series

At present there are two published standards in information security family: ISO/IEC 27001:2005 "Technology – Security techniques –Information security management requirements", and ISO/IEC 17799:2005 "Information Technology – Security techniques – Code of practice for information security management".

ISO/IEC 17799:2005 is a direct descendant of the British Standard Institute (BSI) Information Security Management standard BS 7799. The BSI (www.bsi-global.com) has long been proactive in the evolving arena of Information Security.

In response to industry demands, a working group devoted to Information Security was first established in the early 1990's, culminating in a "Code of Practice for Information Security Management" in 1993. This work evolved into the first version of the BS 7799 standard released in 1995.

In the late 1990's, in response to industry demands, the BSI formed a program to accredit auditing firms, or "Certification Bodies," as competent to audit to BS 7799. This scheme is known as c:cure. Simultaneously, a steering committee was formed, culminating with the update and release of BS 7799 in 1998 and then again in 1999. The BS 7799 standard now consists of Part 1: Code of Practice, and Part 2: Specification of Information Security Management Systems.

---

[2] Jacobson, R. (2002). Quantifying IT Risks. Retrieved August 30, 2006, from http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=479

By this time, information security had become headline news and a concern to computer users worldwide. While some organizations utilized the BS 7799 standard, demand grew for an internationally recognized information security standard under the aegis of an internationally recognized body, such as the ISO. This demand led to the "fast tracking" of BS 7799 Part 1 by the BSI, culminating in its first release by ISO as ISO/IEC 17799:2000 in December 2000. As of September 2001, only BS 7799 Part 1 has been accepted for ISO standardization because it is applicable internationally and across all types of organizations. Movement to submit BS 7799 Part 2 for ISO standardization has been withdrawn. The revised version of ISO/IEC 17799:2000 was published on the 15th June 2005. Now that the 2005 version is officially published the 2000 version has been withdrawn. The new version of ISO/IEC 17799:2005 is still just a Code of Practice, defining best practice controls. It still uses only the word 'should' in all of its controls, leaving the selection of controls and their implementation entirely up to the organization – compare this with BS 7799 Part which is a requirements specification and uses the word 'shall' in all its controls enabling users to use it for accredited certification purposes.

ISO/IEC 27001:2005 was published on the 15th October 2005. This Information security management system requirements standard replaces BS 7799 Part 2:2002 and the latter is now withdrawn.

2.4 ISO/IEC 17799:2005, Code of Practice for Information Security Management

ISO/IEC 17799:2005 is set of guidelines and general principles used for initiating, implementing, maintaining, and improving information security management in an organization. Objectives mentioned in this standard supply general guidance for information security management goals which are generally accepted.

According to the standard itself, after a risk assessment process some requirements are identified. The control objectives and controls that exist in this standard are intended to be implemented to meet these requirements. In addition this standard can be used as a guide to develop organizational security standards and effective security management practices and to help build confidence in inter-organizational activities [1].

This standard is preferably used in conjunction with ISO/IEC 27001:2005, which is a specification for an information security management system, how to set it up and work it. In short it is easily to say that ISO/IEC 27001:2005 covers how to set up and organize the work towards information security, and ISO/IEC 17799:2005 provides a comprehensive set of best practices from which organization has to choose those that apply to the organization. As a requirement in annex A of ISO/IEC 27001: 2005, it is stated that organization has to go through ISO/IEC 17799: 2005 and decides which controls organization needs and does not need to implement.

ISO/IEC 17799:2005 offers a range of high-level guidelines, controls and "best practices" for security management within 11 different areas collectively containing a total of 39 main security categories and one clause which introduces risk assessment and treatment. Currently these areas cover:

- Security Policy (1)
- Organizing Information Security (2)
- Asset Management (2)
- Human Resources Security (3)
- Physical and Environmental Security (2)
- Communications and Operations Management (10)
- Access Control (7)
- Information Systems Acquisition, Development and Maintenance (6)
- Information Security Incident Management (2)

- Business Continuity Management (1)
- Compliance (3).

Each main security category contains:

- a control objective stating what is to be achieved and
- one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:
Control defines the specific control statement to satisfy the control objective.

Implementation guidance provides more detailed information to support the implementation of the control and meeting the control objective. Some of this guidance may not be suitable in all cases and so other ways of implementing the control may be more appropriate.

Other information provides further information that may need to be considered, for example legal considerations and references to other standards [1].

It is not an obligation to comply with all of the 133 controls, only those considered relevant, but it shall be explained why those are chosen and why the others are left out. Most organizations will probably never feel that they need, or have use of, all the controls, but every organization should be able to find all the controls they need in the standard.

2.5 ISO/IEC 27001:2005, Information Security Management Requirements

Information security defects can cause financial loses and breakdown of business operations. The newly published ISO/IEC 27001:2005 standard for information security management systems can help organizations plug existing leaks and prevent future threats that can prove to be extremely damaging and harmful.

Basically, ISO/IEC 27001:2005 sets out the requirements for how an organization can implement the security requirements of ISO/IEC 17799:2005. The aim of ISO/IEC 27001:2005 is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS.

According to the Standard, an ISMS is defined as:

"The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources." [2] In other words, the ISMS encompasses the entire information security program of an organization, including its relation to other parts of the organization. While ISO/IEC 27001:2005 does not provide a complete prescription for a proper information security program, it does list the various organizational functions required for certification, including a list of required documents that must be produced.
The OECD has also shown interest in information security. The guideline "OECD Guidelines for the Security of Information Systems and Networks towards a Culture of Security" has been issued [8]. ISO/IEC 27001 uses a process-based approach, copying the model defined by the OECD.

ISO/IEC 27001:2005 uses process approach for the management of information security. This approach encourages users to emphasize the importance of:

- Understanding the need for information security policy and objectives and deciding information security requirements for the organization
- Implementing and operating safeguards in order to mitigate the organization's information security risks in line with the organization's overall business risks
- After establishing the ISMS, monitoring and reviewing the performance and effectiveness of it
- And lastly, continual improvement based on objective measurement [2].

The Plan-Do-Check-Act (PDCA) Approach [8], which is applied to structure all ISMS processes, breaks overall organizational processes into four phases, as shown in Figure 2.

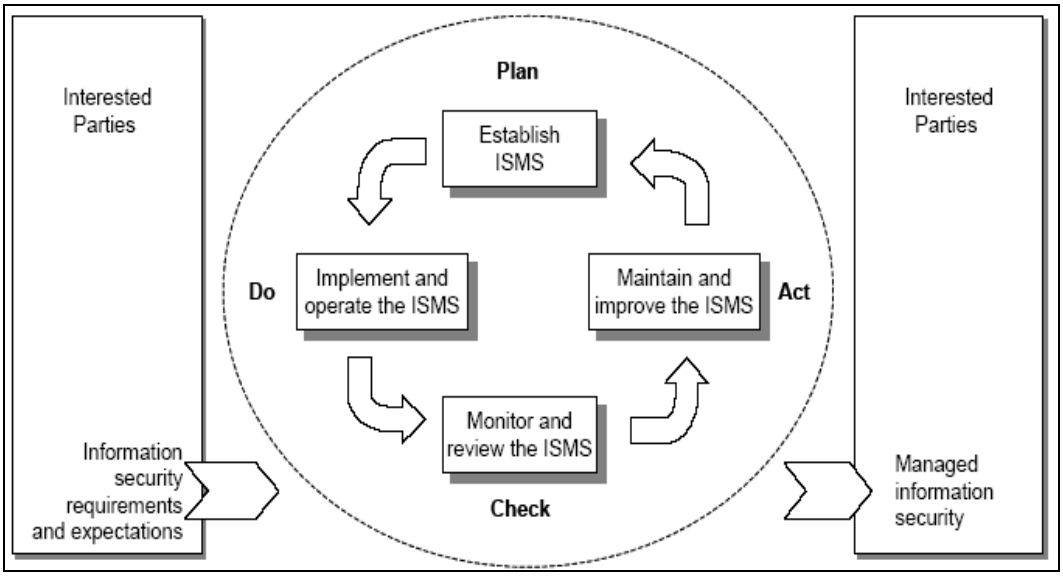


Figure 2 – PDCA model applied to ISMS processes

ISMS is a proactive approach to continuously and effectively manage, at a high level, information security including people, infrastructure and businesses. The goal is to reduce risks to manageable level, while taking into perspective both business goals and customer expectations.

ISMS is not specific to an industry. The beauty is that the concepts from ISMS can be applied with little modifications to make it relevant to a specific industry. ISMS is not a specific virus update, or a patch or a firewall rule set, but it is the common sense behind what needs to go where. Many enterprises already have significant investment in information security products such as firewalls and anti-virus. ISMS maximizes the efficient use of all the organizational resources.

The ISMS is intended to be used by organization management to control and minimize the information security related risks. Important steps in the ISO/IEC 27001:2005 process are:

- Plan (establish the ISMS): Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives [2].
    - SCOPE: Define the scope of the ISMS.
    - ISMS POLICY: What will be accomplished? What is needed to accomplish the security objectives?
    - RISK ASSESSMENT: What are the actual risks? Which risks are acceptable and which are not?
    - RISK TREATMENT: How will be the risks treated?
    - SELECT CONTROLS: Which of the controls in ISO/IEC 17799:2005 is needed to implement? Which are relevant?
    - STATEMENT OF APPLICABILITY: Explanations of reasons for selected and excluded controls.
- Do (implement and operate the ISMS): Implement and operate the ISMS policy, controls, processes and procedures.
- Check (monitor and review the ISMS): Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- Act (maintain and improve the ISMS): Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

2.6 Adoption of ISO/IEC 27001:2005 and ISO/IEC 17799:2005

According to 2005 CSI/FBI Computer Crime and Security Survey, the top five security areas which respondents identify as important, security policy (77

percent), network security (76), security management (72 percent), and access control systems (67 percent) were also among the security areas identified by last year's respondents as an area in which security training is important [9]. Namely, management issues about information security have utmost importance according to the respondents to the CSI/FBI survey. One of the best ways of achieving management issues of information security is adoption of ISO/IEC 27001:2005 and ISO/IEC 17799:2005.

Nowadays number of organizations around the world using these standards is increasing. When an organization recognizes ISO/IEC 27001:2005 as a business objective, one of the first decisions that the organization should consider is whether to simply achieve compliance or attain formal certification.

Certification is only achievable against ISO/IEC 27001:2005, not ISO/IEC 17799:2005. Since the latter is 'code of practice' it is not possible be audited against it. Achieving certification to ISO/IEC 27001:2005 achieves compliance to ISO/IEC 17799:2005 also, because it will be necessary to use ISO/IEC 17799:2005 extensively in deciding on the detailed measures appropriate to each control.

The main difference between certification and compliance is the requirement for a formal audit for certification, which is carried out by an independent auditor. Certification allows the organization to proclaim the achievement of the standard and therefore the effectiveness of their information security.

According to the "Information Security Breaches Survey 2006 - Technical Report" BS 7799 (BS 7799 Part 1 became ISO/IEC 17799 in 2000; BS 7799 Part 2 became ISO/IEC 27001 in 2005) adoption helps organizations become more commercially acceptable to the public sector. In addition, Nine-tenths of businesses that have implemented BS 7799 believe that they obtain benefits from it. The most common benefits are raising staff awareness and pushing security higher up the management agenda. Nearly a quarter of large businesses cited better business continuity as the

biggest benefit. Formal accreditation and marketing was not normally the main benefit, except in very large companies. This may explain why formal accreditation rates remain very low in the UK compared with some other countries [10].

In Table 1 below, the certificates distribution per country is given. The register at the International ISMS User Group, where companies themselves report that they have been certified, had an "Absolute Total" of 2830 certifications worldwide as of August 2006. The total number of ISO/IEC 27001 certificates is now 287 (this includes 112 BS 7799 Part 2:2002 upgrades and 175 new certifications). The Absolute Total represents the actual number of certificates.

Table 1 – Number of Certificates per Country [3]

Japan	1715	Ireland	11	Denmark	2
UK	262	Austria	9	Slovak Republic	2
India	201	Sweden	9	South Africa	2
Taiwan	94	Spain	8	Sri Lanka	2
Germany	62	Turkey	7	Armenia	1
Italy	42	Iceland	6	Chile	1
USA	42	Greece	5	Egypt	1
Korea	38	Kuwait	4	Indonesia	1
Hungary	31	Mexico	4	Lebanon	1
China	28	Russian Federation	4	Luxemburg	1
Netherlands	28	Saudi Arabia	4	Macedonia	1
Singapore	24	UAE	4	Morocco	1
Hong Kong	22	Argentina	3	New Zealand	1
Australia	20	Canada	3	Pakistan	1
Czech Republic	16	France	3	Peru	1
Finland	15	Isle of Man	3	Qatar	1
Poland	15	Slovenia	3	Romania	1
Norway	14	Bahrain	2	Serbia and Montenegro	1
Malaysia	13	Belgium	2	Thailand	1
Switzerland	13	Colombia	2	Vietnam	1
Brazil	11	Croatia	2	***Total***	***2830***

[3] "ISMS Certificates", Retrieved August 22, 2006, from http://www.iso27001certificates.com/

The total number of BS 7799 Part 2:2002 certificates is 890 on October 8th, 2004 [11]. The number of certificated companies is tripled in less then 2 years. Japan is the leading country and provides approximately 60% of all the certifications as in 2004. It is interesting that one of the biggest industrial nations, USA, only has 42 certifications, equaling to around 1.4% of the total. Anyway while the number of certifications was only 9 in 2004; the number has been increased to 42 in 2006.

The reason why the situation looks like that may be described as America has not yet grasped the urgency of the problem. Or most of the organizations in US focus their resources and efforts to regulatory requirements instead. Maybe business value of pursuing formal ISMS certification has not been understood sufficiently. Anyway while the number of certifications was only 9 in 2004; the number has been increased to 42 in 2006.

The people at http://www.gammassl.co.uk/ describe the growth of BS7799-2 (BS 7799 Part 2 became ISO/IEC 27001 in 2005.) with the following self explanatory figure:

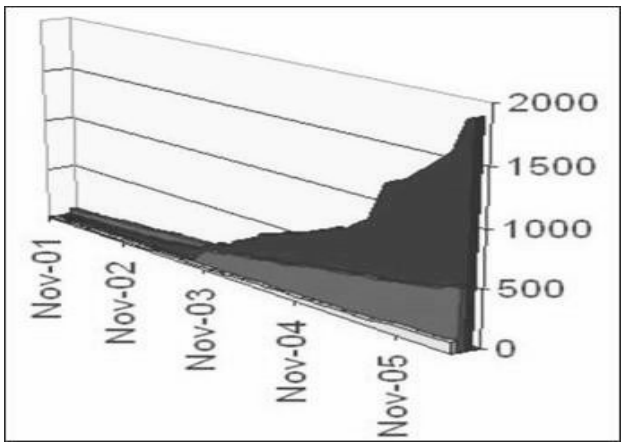


Figure 3 – Growth of ISMS Registrations World Wide [4]

Rest of the World ☐ Europe ■ Asia ■

[4] "The growth of BS7799-2 (BS 7799 Part 2 became ISO/IEC 27001 in 2005.)", Retrieved August 02, 2006, from http://www.gammassl.co.uk/

Nobody knows exactly the number of certifications worldwide as it is optional to report the organization's certification, but what is certain is that the number is growing. As it is seen form Figure 3 above, while more organizations adopt these standards and certifies themselves against ISO/IEC 27001:2005, the growth speed is more exponential.

The situation in Turkey is not different from world's trend. While there is no company certificated in 2004; the number of certificated company is 7 in 2006 in Turkey. It can be said that although it is a new issue for Turkish organizations; it arouses more and more interest. Below Table 2 shows the organizations having ISMS certificates in Turkey including organizations not counted in the Table 1 above.

Table 2 – Organizations certificated against BS 7799-2:2002/ISO/IEC 27001:2005 in Turkey [5]

Name of the Org.	Cert. No.	Cert. Body	Standards
Beko Elekronik A.S.	GB05/64028	SGS Group	BS 7799-2:2002
E-Kart Elekt. Kart Sis. San. ve Tic. A.Ş	192589	BVQI	ISO/IEC 27001:2005
IGDAS	CQ 2184	BVQI	BS 7799-2:2002
Siemens Business Services A.Ş.	GB05/64029	SGS Group	BS 7799-2:2002
Tübitak UEKAE	GB05/65232	SGS Group	BS 7799-2:2002
Turk Traktor ve Ziraat Mak. A .Ş.	IS 96691	BSI	ISO/IEC 27001:2005
TÜRKTRUST Bilgi, İletişim. ve Bilişim Güv. Hiz. A.Ş.	GB05/65355	SGS Group	ISO/IEC 27001:2005
SPK Bilgi Işl. ve Enfor. Da.*	BY -003/06	TSE	TS – ISO-IEC-27001
Plastikkart Ak. Kart. İlet. Sis. San. ve Tic. A.Ş. *	BY-005/6	TSE	TS – ISO-IEC-27001
Simetri Yzl. Tic. Ltd. Şti. *	BY-002/06	TSE	TS – ISO-IEC-27001
Elektronik Bilgi Güvenliği A.Ş. *	BY-001/05	TSE	TS – ISO-IEC-27001
EBG Bilişim Tekn. Ve Hiz. AŞ. *	BY-004/06	TSE	TS – ISO-IEC-27001

[5] "ISMS Certificates in Turkey". Retrieved August 22, 2006, from http://www.iso27001certificates.com/

The total number of ISO/IEC 27001 or BS 7799-2:2002 certificates are now 12 in Turkey. (NOTE: In Table 2 records marked with * are taken from the conversation with Ayşegül İbrişim from TSE)

There are some studies made in METU in this scope, including Master of Science or doctorate theses [18], [19]. Most of these studies are aimed to help securing information systems. However, scope of this thesis is totally different from these studies. After establishing information security system in an organization, studies mentioned above can be used to secure information systems existing in the organization.

2.7 Automated Tools

An organization deciding to adopt ISO/IEC 27001:2005 has to perform the following issues:

- Defining the scope and business requirements, policy and objectives for the ISMS
- Developing an ISMS asset inventory
- Carrying out an ISMS risk assessment
- Facilitating the risk decision process by consideration of the appropriate risk treatment option
- A process for selecting a system of controls
- A documentation facility for producing, for example, a "Statement of Applicability" and other ISMS documents.

The following tools are developed to help or guide organizations whether deciding compliance or certificate in the scope of Information Security in order to perform the issues mentioned above. The tools are described in a general manner what they do and in which Information Security process they fulfill what functionalities.

2.7.1 Callio Secura 17799 [6]

Callio Secura 17799 software was prepared in order to help organizations to conform to the BS 7799/ISO 17799 standard concerning information security management.

It has two separate modules which helps organization's to implement the ISO/IEC 17799 standard and progress toward certification. These are Risk evaluation and Documentary management modules.

First module is Risk evaluation module. This module's aim is to enable managers to manage the level of risk related to each information asset. This module uses qualitative methodology as a risk methodology. First, this module enables users to identify their assets and then evaluate their assets and their associated risks. At the end of this step, users can generate a security policy.
The other module is Documentary management module. This module is used for managing organization's policies and procedures in a systematic and standardized manner. Policies and procedures can be created, modified, and reviewed by this module.

2.7.2 Cobra (Consultative, Objective and Bi-functional Risk Analysis) [7]

Cobra is the abbreviation of Consultative, Objective and Bi-functional Risk Analysis. Cobra was designed to give organizations the means to perform a self-assessment of their security posture without the need for external assistance from consultants. It also helps organizations view information security as a business issue rather than primarily as a technical one.

---

[6] "Callio Secura 17799", Retrieved August 22, 2006, from http://www.callio.com/bs7799/id,301

[7] "Features" C & A Systems Security, Retrieved August 06, 2006, from http://www.riskworld.net/advantages.htm and http://www.riskworld.net/7799.htm

Cobra follows the guidelines stated by ISO/IEC 17799:2005. Cobra's methodology is not a documented process which is the drawback of it. It has two major modules: Risk Consultant and ISO Compliance. Both sub-modules are customizable and utilize knowledge bases containing expert knowledge to aid the user in analyzing their security risks. The users can build their own custom questionnaires based on templates and then use the questionnaire to build a response set. Cobra can produce reports which review and summarize the data and which provide recommendations based on best practices.

Risk Consultant has standard questions. These questions are used to gather information about the organization such as types of assets, vulnerabilities, threats, and controls that are in place in this organization. In addition, the responses given these questions can be used to produce an analysis of the risks, including what-if scenarios, and recommendations for action.

Compliance comes with standard questions which assess the major categories specified in the ISO/IEC 17799:2005 standard. As in Risk Consultant, ISO Compliance can provide an assessment of organizations compliance and suggestions for action.

2.7.3 RA2 Art of Risk [8]

RA2 Art of Risk is a tool to support the application of BS 7799-2:2002 (which was the ancestor of ISO/IEC 27001:2005) by leading the user through the various risk assessment and management processes described in BS 7799-2:2002 (which was the ancestor of ISO/IEC 27001:2005).

[8] "RA2 art of risk", Retrieved August 22, 2006, from http://www.bsi-global.com/ICT/Security/bip0022.xalter

RA2 Art of Risk contains the following modules representing BS 7799-2:2002 (which was the ancestor of ISO/IEC 27001:2005) processes of risk assessment and management.

Information Gathering Module: Here, users can identify the ISMS scope, document and record numbers for the documents, risk policy and objectives, risk assessment scales, assets in the ISMS, business, legal and statutory requirements for the assets. And then the values of the assets and the assets' needs for confidentiality, integrity, availability and other security properties are defined.

Risk Identification and Assessment Module: Here, the threats and vulnerabilities for the assets are identified, in addition in order to express the possibility of the threats and vulnerabilities occurring values of them are identified, and lastly the risks, based on the results of the previous process, are calculated.

Risk Management Decisions Module: Here, the decision for the appropriate risk treatment option is made for the identified risks, control objectives and controls are identified, the risk reduction achieved by the selected control objectives and controls is assessed, and lastly the Statement of Applicability is produced.

Implementation of Controls Module: Here, the implementation of selected controls can be planned. This is a gap analysis against the controls in ISO/IEC 17799:2005, which can be performed to identify their current implementation status.

2.7.4 SecureAware 3.0 Information Security Management System [9]

SecureAware ISMS is a comprehensive information security management system. SecureAware ISMS is a bundle of five modules these are: SecureAware Risk, SecureAware Compliance, SecureAware Policy, SecureAware Survey, and SecureAware Education.

---

[9] "SecureAware® ISMS", Retrieved August 22, 2006, from http://www.neupart.com/

SecureAware Risk Module: SecureAware Risk is a risk assessment and analyses (RAA) tool for commercial businesses and government agencies. The outcome of this process is information security overview of the organization.

SecureAware Compliance Module: This module has built-in compliance checklist which follows ISO/IEC 27001:2005 and ISO/IEC 17799:2005. It also includes questions for specific controls and implementation guidelines. It has a role-based user management ensuring only designated staff can view assessment. It allows linking of related documentation to related references. And lastly, it has a report capability which produces both executive summary and detailed report of compliance status in PDF format.

SecureAware Policy Module: In this module, security policies, procedures and guidelines can be created, maintained and communicated. This tool enables the organization to structure and target the content of pre-defined security policy and to convert content of the organization's pre-defined security policy into awareness programs with SecureAware Survey Module and SecureAware Education Module automatically. In order to establish a security policy all relevant content is included in SecureAware ISMS.

SecureAware Survey Module: This module is designed for ongoing measurement of the human security awareness level. This module evaluates the information security knowledge of the organization's staff and tests their understanding of the security policy and rules of the organization. Based on this information, a custom-tailored security training program can be delivered and evaluated on a regular basis. The integration between Policy, Education and Survey modules enables automatic creation of awareness quizzes based on the organization's specific policies.

SecureAware Education Module: This module makes it possible to educate all employees in security on the exact level relevant for any particular group of

employees. This module is e-learning based security education. The courses particularly focus on teaching in the areas where SecureAware Survey has found weak spots in the knowledge level.

2.7.5 AMS9000 [10]

NOWECO created JKT9000 software for quality management in 2001. JKT9000 is a software family with tools for document control, audit management, corrective actions, and control of non-conforming materials fully complying with ISO9000.

As part of the JKT9000 family of management software modules, AMS9000 is the audit management software. This program is designed to handle all aspects of an internal audit program, from planning audits to the follow-up of corrective actions against deficiencies found.

AMS9000 can be used to verify compliance with any kind of standards including ISO/IEC 17799:2005 and BS 7799.

2.7.6 Risk Register: Risk Assessment Software for ISO/IEC 17799/BS 7799 [11]

Risk Register risk management software package is used to manage general organizational risks related to people, property, reputation, assets and the environment. Hence, it is suitable to manage risks as required in ISO/IEC 17799/BS 7799.

It is based on the joint Australia/New Zealand Risk Management standard AS/NZS 4360 that provides a generic framework for establishing the context, identification, analysis, evaluation, treatment, monitoring and communication of risk. Risk

---

[10] "AMS9000 Audit Management Software", Retrieved August 22, 2006, from http://www.noweco.com/smhe.htm

[11] "Risk Register: Information Security Management", Retrieved August 22, 2006, from http://www.noweco.com/ismse.htm

Register also meets the risk management requirements of many other international standards including ISO/IEC 17799 and BS 7799. Using this tool user can identify, analyze and evaluate the risks and select appropriate treatments based on treatments pre-loaded by risk managers for the identified risks. User also has some capabilities to add short descriptions, hyperlinked documents, due dates etc. to the selected treatment option. User also is able to select the most cost effective treatments at the risk level, at the project or asset level, or at the department, division or organization levels. In addition, all the risks and the treatments are assigned to someone so that owners can be notified when risk reviews and treatment actions are due, and escalates to authorized officer if overdue. This tool also enables managers to assess all risks by risk category, project, asset, department, division or organization wide. And lastly, this tool provides insight into the effectiveness of the risk management process by project, asset, department, division and location.

2.7.7 CRAMM v5.1 Information Security Toolkit [12]

CRAMM contains a database consisting of over 3,500 security controls. It has also a set of tools to support users in achieving certification or compliance against BS7799: 2005/ISO/IEC 27001:2005. It has pre-defined information security policies, security operating procedures and other useful security documentation and risk assessments covering generic information systems – such as payroll. And lastly it has a risk management help tool which supports organization's security improvement planning and makes the most of the information security budgets.

CRAMM provides a staged approach embracing both technical and non-technical aspects of security. In order to assess these components, CRAMM is divided into three stages:

- Asset identification and valuation

[12] "Risk Assessment Tool", Retrieved August 22, 2006, from http://www.cramm.com/capabilities/risk.htm

- Threat and vulnerability assessment
- Countermeasure selection and recommendation

In addition, it supports some additional functions including:

- BS7799: 2005 Compliance
- Production of Security Documentation
- Investigation against Standards
- Recording information required for Business Continuity Planning.

2.7.8 MSAT (Microsoft Security Assessment Tool) [13]

The Microsoft Security Assessment is designed to help customers understand their security gaps and risks. MSAT is an interactive session that includes an on-site questionnaire and can last from one to two hours. It is a repeatable, scalable, and predictable tool.

MSAT includes a detailed questionnaire assessing multiple areas of the organization. When finished, MSAT generates a comprehensive report which can be used to get an overall view of the organization's security situation and identify specific areas of the organization where security is at a mature and strong level.

2.7.9 Pirean-Policybase [14]

This tool is created for policy and procedure administration. Policybase enables users to centrally and securely store all their organization's information security policies and procedures. It ensures that all the organizations' policies are version controlled, secure, available, have complete integrity and are up-to-date, as well as giving users an automated workflow through an online approval and distribution

---

[13] "How secure is your business?" , Retrieved August 22, 2006, from http://www.microsoftsecurityassessment.com/

[14] "Policybase Pirean Software" , Retrieved August 22, 2006, from http://www.pirean.com/technology/?SubSectionID=24/

system. It ensures the organization's staff understands their responsibilities and commitments to the organization which is essential to the success of the organization.

2.7.10 RiskWatch for Information Systems & ISO/IEC 17799 [15]

RiskWatch for Information Systems & ISO/IEC 17799 is used for conducting IT risk analyses and vulnerability assessments. It includes control standards from ISO/IEC 17799, and NIST 800-26. It includes a simple web-based questionnaire application that user can load on their own server and make compliance questions available to system users. Respondents simply answer and return these completed questionnaire files for consolidation and risk analysis. Users may generate an unlimited number of questionnaire sets. The answers are imported back into RiskWatch, analyzed and used to create management level reports.

It includes an Asset Configuration Tool, based on a standard capital expenditures allocation, so that asset information fields can be populated. Default data on threat frequencies, and the cost of applicable safeguards (controls) is included.

The user can customize RiskWatch, create new asset categories, threat categories, vulnerability categories, safeguards, question categories, and question sets. Users can also automatically import questions and data created by other users into their analysis.

Return on Investment is calculated for each safeguard and a Case Summary Report is generated automatically which shows Compliance vs. Non-Compliance, Protection Levels, and Annual Loss Expectancy data by Asset category, threat or loss impact category.

---

[15] "RiskWatch for Information Systems & ISO 17799™", Retrieved August 22, 2006, from http://www.riskwatch.com/products/isa.asp

This tool has one drawback that it is not built for ISO/IEC 27001:2005 just for ISO/IEC 17799:2005.

2.7.11 Praxiom Research Group- ISO/IEC 27001:-2005 Gap Analysis Tool [16]

ISO/IEC 27001: 2005 Gap Analysis Tool is designed for specify what an organization needs to do to comply with the ISO/IEC 27001: 2005 information security management standard. This tool pinpoints the gaps that exist between the new standard and the organization's current security practices. This tool assumes that the organization already has an information security management system (ISMS) and that all the organization needs to do is make incremental changes in order to ensure that it complies with the new ISO/IEC 27001: 2005 standard.

2.7.12 Proteus Enterprise [17]

Proteus Enterprise enables organizations to comply against Standards important to them with a low effort and high confidence. It is designed to integrate organization's information and systems by gathering and reporting on data collected at one or multiple organizational areas and/or locations. This tool has two modules. These are Proteus Compliance Module and Proteus Manager Module.

Proteus Compliance Module: This module enables easy gap analysis to be conducted against a chosen standard such as BS 7799/ISO/IEC 17799. It fully supports questionnaire authoring including customized weighting of questions, risk ranking of controls and automatic linking to generic implications and deliverables from control deficiencies.

---

[16] "ISO IEC 27001 2005 INFORMATION SECURITY GAP ANALYSIS TOOL", Retrieved August 22, 2006, from http://www.praxiom.com/iso-27001-gap.htm

[17] "Proteus Enterprise", Retrieved August 22, 2006, from http://www.infogov.co.uk/

Proteus Manager Module: This module allows the creation and management of an ISMS according to BS 7799 Part 2 (which was the ancestor of ISO/IEC 27001:2005). It is designed to be used in combination with Proteus Compliance software. Proteus Manager is designed around processes defined by the BS 7799 Part 2 (ISMS) Standard but it can be used as a generic Policy Management tool.

Proteus Manager enables organization's assets to be dynamically linked to specific security controls in the Proteus Compliance module. Furthermore, controls can be associated directly to individuals.

In addition to these two modules' functionalities, Proteus Enterprise has a report designer that satisfies the most demanding of reporting requirements. Moreover, deficiencies are dealt with quickly and concisely using the workflow management. And lastly, Proteus Enterprise promotes ownership of problems and maintains accountability throughout the enterprise.

2.7.13 ISMart Information Security Management Software [18]

ISMart Information Security Management Software has been developed by BizNet for organizations that need to establish and maintain an ISMS according to BS 7799 specifications. This tool enables organizations to manage their risks, automatically generate their policy documents, measure effectiveness of ISMS, manage security incidents, and generate all necessary reports. ISMart is the first tool which was developed in Turkey for Information Security Management. This software has the following modules:

Risk Analysis and Management Module: This module provides the capability of establishing and management of risk management system.

---

[18] "ISMart Bilgi Güvenliği Yönetim Sistemi Yazılımı", Retrieved August 22, 2006, from http://www.biznet.com.tr/ismart_info.htm

Document Management Module: Using this module system documentation in accordance with the standard requirements can be produced and managed. The existing database contains predefined asset categories, threats and controls, which will make risk analysis as simple as creating assets under an appropriate asset category. The organizations can tailor this database to create their own asset categories, threats and control assignments according to their needs.

Gap Analysis Module: This module provides the ability of constituting and monitoring awareness level in the organization. Questionnaires for measuring how far the organization is from compliance can be created and forwarded. And the organization's awareness level can be measured.

Management Module: This module gives a web based management interface that provides usage flexibility.

In addition to the modules' functionalities, ISMart provides scalable solution that fits into even the biggest organization. And with ISMart, security incidents can be tracked and resolved seamlessly. And lastly, ISMart automatically creates all necessary reports: inventory, risk, risk treatment, SOA etc.

2.7.14 EAR Environment for the Analysis of Risk [19]

EAR provides a set of tools for analysis and management. It supports the methodology Magerit provided by the Spanish Administration.

EAR uses a general purpose library for assets, threats and safeguards. Furthermore, it is able to derive security qualifications against widely known security standards, such as ISO/IEC 17799:2005: Code of practice for security information security management.

---

[19] "Environment for the Analysis of Risk", Retrieved August 22, 2006, from http://www.ar-tools.com/en/index.html

This tool enables organizations to identify, classify, relate and evaluate their assets. And then the organization can identify and evaluate threats on the identified assets. And the controls can be identified and evaluated either already in place, or to be deployed as part of a security plan. This tool also helps to create a disaster recovery plan.

2.7.15 ISMS Tool Box [20]

The ISMS Tool Box enables organizations to develop, operate and maintain an Information Security Management System. It allows the organization to create rules and regulations and to communicate them in different languages through the intranet. Organization's existing rules and regulations can be integrated. In a working group the rules and regulations can be reviewed and validated and their implementation planned and continuously monitored.

This tool enables the organization to assign all the assets to someone and identify and classify the assets. It enables users to execute risk analysis and also to develop and compile individual analyses. Organization can create implementation plan based on the compliance analysis. On the intranet all internally used abbreviations and security relevant terms are easily available and explained. In addition, it allows direct intranet based access to ISO/IEC17799/BS7799, COBIT, IT-Grundschutzhandbuch of BSI Germany and the Swiss Infosec Baseline Catalogue. And lastly, it allows compilation of reports for all the security measures.

2.7.16 Asset Track [21]

Assettrack is software which helps in accumulating and managing the information & documentation required for ISO/IEC 27001:2005. It is a web based application which can be used by multiple users. Since it can be used across an organization

---

[20] "ISMS Tool Box", Retrieved August 22, 2006, from
http://www.ismstoolbox.com/index.asp?lang=en

[21] "Risk Assessment tool for ISMS", Retrieved August 22, 2006, from
http://www.libsuite.com/asset_track.htm

and hence it supports handling of multiple locations within an enterprise. Assettrack has two main modules. These are Document Management Module Asset Management Module.

Document Management Module: This module enables user to create a repository of some documents, which are required for the ISMS process, such as policies, control documents, Statement of Applicability, organization structure, information classification etc. In addition it offers a facility for maintaining the version control for the revisions uploaded.

Asset Management Module: This module enables user create assets according to their category and thus create an Asset Repository. This tool has also a capability to generate for each asset. It has a sub module which can be used for risk assessment and risk treatment. In addition it allows defining various threats and various vulnerabilities associated with those threats. This is done by creating a repository of vulnerabilities. And lastly it has some reporting capabilities.

2.8 Automated Tools Comparison

There are various tools developed in order to help organizations during the ISMS process or in a general manner for information security issues. There are not so many tools helping organizations to construct the information security or to establish an ISMS as a complete manner. Table 3 presents a simple comparison of specific tools which helps organizations in one or more areas and the project InfoSec Toolkit developed in the context of this thesis.

As it is clearly seen from Table 3 most tools concentrates on one or several specific area. Most of them concentrated on a specific scope of information security. Although using a tool which concentrates on a specific area can be useful, but using a more comprehensive tool which helps in all aspects of information security and ISMS process can be more advantageous.

Table 3 – Comparison of Information Security Tools

ISMS Tools						
No	Name	Risk Man.	Policy Man.	Gap Analysis	Monitoring Module	Awareness & Education Module
1	Callio Secura 17799	X	X	X	-	-
2	Cobra (Consultative, Objective and Bi-functional Risk Analysis)	X	-	-	-	-
3	RA2 Art of Risk	X	-	X	-	-
4	SecureAware	X	X	X	-	X
5	AMS9000	-	-	-	X(Audit)	-
6	Risk Register	X	-	-	-	-
7	CRAMM v5.1 Information Security Toolkit	X	X	X	-	-
8	MSAT (Microsoft Security Assessment Tool)	-	-	X	-	-
9	Pirean-poicybase	-	X	-	-	-
10	RiskWatch 17799	X	-	X	-	-
11	Praxiom ISO 27001:2005 Gap Analysis Tool	-	-	X	-	-
12	BizNet	X	X	X	-	-
13	ISMS Tool Box	X	X	-	-	-
14	Proteus Enterprise	X	X	X	-	-
15	EAR (Environment for the Analysis of Risk)	X	-	-	-	-
16	Asset Track	X	X	-	-	-
17	InfoSec Toolkit (the proposed system)	X	X	X	X	-

In addition there is no tool developed in Turkish except BizNet's ISMart. Since our aim is to contribute Turkish organizations in the information security field, usability of the tools used by Turkish organizations is important. And considering the growth rate of interest in information security's management aspect, it can be stated that the number of tools especially developed in Turkish thus used by Turkish organizations easily is limited. So it is important for Turkish organizations to have a tool having Turkish interfaces.

And lastly, as seen in the table above, except AMS9000, which provides only audit capability, none of the tools has monitoring capabilities. However, one of the main differences of the project InfoSec Toolkit from other tools is to enable organizations monitor their information security status after the establishment of ISMS periodically or as necessary.

CHAPTER 3

APPROACH

3.1 Purpose and Scope

The approach, of which the details were given in section 2.5, adopted by ISO/IEC 27001:2005 forms the basis of this thesis' approach. The general purpose of the approach, adopted by the thesis, is to help organizations throughout the process of establishing, implementing, operating, monitoring, reviewing, maintaining and improving their ISMS by automating the process as much as possible. This approach consists of five main modules; Initial Gap Analysis, Risk Management, Policy Management, Monitoring and the ability of inquiry and report on information generated during other operations. Initial Gap Analysis provides a means to help organizations to take the picture of their current situation of Information Security status before the beginning of establishing the ISMS. Risk Management enables the organizations to implement the requirements of Plan and Do phases, as specified in section 2.5. These requirements are Definition of the ISMS Scope, Creation of Assets in the ISMS, Determining the Valuation of Assets, Identification of Threats and Vulnerabilities, Risk Identification and Assessment, Deciding Risk Treatment Options and Generating some required documents such

as Risk Assessment Report, Risk Treatment Plan, Asset Inventory, and Statement of Applicability and so on. Policy Management helps organizations to specify polices and procedures governing the implementation of the controls selected in order to reduce information security risks to an acceptable level. Monitoring gives a means to help organizations monitor the ISMS and review it periodically or in case of need and then decide the required arrangements in order to improve the ISMS, after the establishing the ISMS. This approach includes a report generation and query system which uses historical data generated throughout the processes in order to give opportunity to the organizations' managers to comprehend their ISMS situations.

In addition, this approach includes a research framework which can be used to take the picture of Information Security levels of organizations. This framework not only includes an evaluation methodology but also includes a report generation system which uses historical data for reports to indicate comparative situation of different organizations either in a specified scope of business or a specified sector. In addition, a report, which takes the picture of current situation about Information Security and gives advices in order to strengthen the foibles of the organization, can be generated for a particular organization.

3.2 Assumptions and Dependencies

ISO/IEC TR 27001:2005 dictates organizations to identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements [2]. For risk management issue, ISO/IEC TR 27001:2005 refers ISO/IEC TR 13335-3:1998 which discusses the examples of risk assessment methodologies [2]. Although this standard says that organizations select a risk assessment methodology that is suited to their ISMS, this approach uses Detailed Risk Analysis. Although the decision to use a quantitative based scale versus a qualitative scale is really a matter of organizational preference,

this thesis adopts an approach in which qualitative scale is used in order to evaluate the assets [12].

The approach by its nature has a sequential and cyclic structure because of the process approach. It is assumed that users shall use the system successively namely, firstly Initial Gap Analysis Module, secondly Risk Module, thirdly Policy Management Module and lastly Monitoring Module. On the other hand query and reporting capabilities can be used in case of need.

It is assumed that within the organization one or more ISMS shall be established. These ISMS information shall be stored on a specified database. Only completed evaluation results shall be included in report generation phase.

3.3 Initial Gap Analysis

ISO/IEC 27001:2005 and ISO/IEC 17799:2005 require a careful interpretation for current organizational environments and the organization's information security posture before beginning the establishment of ISMS. These standards provide an important authoritative statement for senior management, and extensive checklists of security measures. Security officers of the organizations should submit an initial report generated by using these checklists for senior management. This initial report should have details about the organizational level of information security management is, or is not, consistent with guidelines [13]. This approach will help to generate this initial report. Initial Gap Analysis consists of two sets of questionnaires. These are ISO/IEC 27001:2005 Information Security Initial Gap Analysis and Assessment of ISMS Process Requirements. These questionnaires are prepared in accordance with "Are you ready for a BS 7799 Audit? (PD 3003)" developed by DISC, the department within BSI that manages the IT and telecommunications standardization. Although this guide is not up to date, it helped constituting the framework for the questionnaires [14].

These questionnaires are used by organizations wishing to carry out initial compliance checks of their ISMS against ISO/IEC 27001:2005 and ISO/IEC 17799:2005.

ISO/IEC 27001:2005 Information Security Initial Gap Analysis is purely a means to confirm what controls are in place in accordance with the requirements specified in ISO/IEC 27001:2005. Where particular control requirements are not completely satisfied, organizations shall document the reasons why they have not been met and the justifications of excluding the control requirements. It contains 11 categories collectively containing a total of 133 security questions. These categories are the security control clauses specified in ISO/IEC 17799:2005 and the questions measure the implementation level of 133 controls contained in these 11 security control clauses.

The other questionnaire is Assessment of ISMS Process Requirements. This questionnaire has 81 questions totally accumulated under 6 categories. This questionnaire checks the ISMS process requirements. It includes establishing that the prerequisite processes and measures defined Clauses 4 to 8 of ISO/IEC 27001:2005 are in place.

These questionnaires can be used not only for initial analysis but also for internal audits during the Check phase.

3.4 Risk Management

Risk Management approach is generally based on ISO/IEC TR 13335-3:1998 and Guide to BS 7799 Risk Assessment (PD 3002).

Risk Management consists of two major activities. These are risk assessment and risk treatment. When bethinking the PDCA Model and the activities to be implemented in the ISMS process, it is clear that risk assessment is a major part of the “Plan” phase and in the same way risk treatment is a part of “Do” phase of

PDCA model. And similarly, re-assessment of all risks to check whether the controls are mitigating the risks effectively is the part of the "Check" phase and treating the re-assessed risks is the part of "Act" phase of PDCA model [14]. In this approach Detailed Risk Analysis is adopted as a risk assessment approach.

3.4.1 Detailed Risk Assessment

In order to understand the risk assessment process, it is essential to describe the term risk. NIST SP 800-30 defines risk as, "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." Namely, where a threat intersects with vulnerability, there occurs a risk. The aim of risk assessment is to identify and assess the risks in a particular environment [15].

The approach adopted by this thesis includes the detailed identification and valuation of assets, and identification and assessment of the levels security requirements. The information generated during the identification assets and requirements is used to evaluate the risks and then for identification and selection of security controls from ISO/IEC 17799:2005.

From a different point of view risk assessments are divided into two groups as Quantitative Risk Assessment and Qualitative Risk Assessment. First one uses quantitative measure and the latter uses qualitative measures. Details of these approaches are given in Section 2.2.

Because of the difficulty in measuring a numerical value for any of these factors, it has been asserted by many experts that a purely quantitative risk assessment is not possible or practical. That is why in this thesis qualitative risk assessment approach is used.

Risk assessment depends on the following factors:

- Identification and valuation of assets

- Identification of all security requirements such as threats and vulnerabilities
- legal and business requirements
- Assessment of the likelihood of the threats and vulnerabilities occurrence
- Calculation of risk resulting from these factors
- Selection of the appropriate risk treatment option
- Selection of controls to reduce the risks to an acceptable level [14].

3.4.1.1 Asset Identification

Prior to identification of assets, the scope of the ISMS is defined in the light of the characteristics of the business, the organization, its location, assets and technology in order to make sure that no asses is forgotten. After defining the scope of ISMS, the next step is to develop an inventory of assets contained in the ISMS, and the owners of these assets.

The asset types used by this approach include:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements
- Software assets: application software, system software, development tools and utilities, e-learning assets, network utilities and services
- Physical assets: computer and communications equipments, magnetic media, other technical equipment such as power supplies, air-conditioning units and furniture
- Services: computing and communications services, other technical services such as heating, lighting, power, air-conditioning
- Human resources: personnel, customers, subscribers
- Company image and reputation.

3.4.1.2 Asset Valuation

Asset identification and valuation is the main part of the risk assessment process. In order to define the proper protection for assets, it is required to evaluate the values

of the assets in terms of their importance to the business. The values assigned to assets are related to the impacts of the loss of confidentiality, integrity and availability to the organization and the cost of obtaining and maintaining the asset. For each of the assets, values are assigned that express the business impacts in case confidentiality, integrity or availability or any other important property of the asset is damaged.

This approach uses the following valuation scale:

- Low (1)
- Low – Medium (2)
- Medium – High (3)
- High (4)

3.4.1.3 Identification of Security Requirements

In this phase of the approach security requirements are identified. Generally no matter what the size of the organization, security requirements are derived from three main sources. These are threats and vulnerabilities, statutory and contractual requirements and the set of principles, objectives and requirements for information processing that the organization has developed to support its business operations.

3.4.1.4 Identification and Assessment of Threats and Vulnerabilities

According to the ISO/IEC 13335-1:2004, assets are subject to many kinds of threats. A threat can cause harm to an asset and consequently can damage organization's business [13]. Threats may be either accidental or deliberate. A threat needs to exploit an existing vulnerability of the asset in order to harm the asset.

Vulnerability is a weakness of asset/s that can be exploited by threat/s [13]. Vulnerability can exist without threats. Vulnerability does not cause harm by itself; it is just a condition or set of conditions that may allow a threat to affect an asset.

According to the adopted approach threats and vulnerabilities are assessed separately. Similar to the valuation of assets, it is required for valuation of treats and vulnerabilities to define a scale for this valuation suitable to the risk assessment approach applied. In order to not make the process complex, for both treats and vulnerabilities assessment the following valuation scale is used.

- Low (0)
- Medium (1)
- High (2)

It is also required to identify security properties (confidentiality, integrity, availability, and any other properties that have been identified for the asset during the asset valuation phase) that relate to the calculated risk of exposure.

3.4.1.5 Calculation of Security Risks

The aim of risk assessment is to define and evaluate the risks based on the results derived from Asset Valuation and Threats and Vulnerabilities Valuation phases. The risk calculation process is explained below.

Two inputs are used in order to calculate the risks for each asset. First one is the business impact that losses of confidentiality, integrity, availability, and a possible other security properties would have on the ISMS assets. And the other one is the risk of exposure level based on the identified threat and the vulnerability values. According to the identified values for the threats and vulnerabilities, corresponding risk of exposure for each threat/vulnerability combination is calculated.

Table 4 – Risk of exposure matrix

		Threat		
Vulnerability		**Low Likelihood (0)**	**Medium Likelihood (1)**	**High Likelihood (2)**
	Low (0)	Very low risk of exp.(0)	Low risk of exposure (1)	Medium risk of exp. (2)
	Medium (1)	Low risk of exp. (1)	Medium risk of exp. (2)	High risk of exp. (3)
	High (2)	Medium risk of exp. (2)	High risk of exposure (3)	Very High risk of exp. (4)

According to the approach, risk calculation formula is as below.

Risk level = Risk of exposure level + Maximum of impact levels for the asset – 1 [16].

Table 5 – Risk matrix

		Risk of Exposure				
Business Impact		**Very Low(0)**	**Low(1)**	**Medium(2)**	**High(3)**	**Very High(4)**
	Low(1)	1	2	3	4	5
	Low–Medium(2)	2	3	4	5	6
	Medium–High(3)	3	4	5	6	7
	High(4)	4	5	6	7	8

After the execution of a detailed risk analysis, the results of the review -asset and their values, threat, vulnerability and risk levels, and safeguards identified - should be saved in a database [12].

3.4.2 Identification and Evaluation of Options for Risk Treatment

Second part of the risk management process is to treat the risks in a proper way. Risk treatment can be described as "the process of selection and implementation of controls to modify risk" [13].

There are four possible actions can be taken by an organization in order to handle a risk. These are:

- Risk avoidance
- Risk transfer
- Risk reduction
- Risk acceptance

3.4.2.1 Risk Avoidance

Risk avoidance describes any action taken to avoid the risk by eliminating the risk cause and/or consequence. To decide not to process sensitive information with third parties is an example of risk avoidance.

3.4.2.2 Risk Transfer

Risk transfer can be described as to transfer the risk by using other options to compensate for the loss. In some circumstances risk transfer might be the best option. For example, if to avoid risk seems impossible, or if it is difficult or too expensive to achieve proper mitigation of risk this option can be selected. Purchasing insurance or using third parties or outsourcing partners to handle critical business assets or processes can be the possibility of risk transferring.

3.4.2.3 Risk Reduction

Risk reduction can be described as limiting the risks by implementing the appropriate controls that minimize the risks to an acceptable level. In order to reduce the risks, where the option 'risk reduction' has been chosen, proper and justified security controls are identified and selected. Controls are selected mainly from ISO/IEC 17799:2005. In addition, controls can be selected from additional resources. The purpose of control selection is to diminish the risks to an acceptable level.

3.4.2.4 Risk Acceptance

After choosing the suitable controls to reduce the risks to an acceptable level, the level of risk reduced is identified. This reduced risk is called residual risk. After the implementation of the selected controls, there will always be residual risks. That's why no system can be made absolutely secure. These residual risks should be categorized as 'acceptable' or 'unacceptable' for the organization. If the residual risk is unacceptable, a decision is made on how to deal with this risk. These actions are part of the "Check" phase in the PDCA.

3.5 Policy Management

According to the ISO/IEC 17799:2005 an information security policy document shall be formed. This policy document indicates the goals of information security. Information Security Policy forms the basis of the process ISMS. Therefore it is the

initial part of establishing the ISMS. Information security policy can be described as a collection of directives, rules and practices. These documents explain how to manage, protect and distribute information in an organization [16].

Principles in the information security policy should be derived from principles of the organization's security policy so that they are consistent with the latter.

In harmony with the information security policy document there should be policy manuals and procedures which support management's assessment of organization's controls selected during the risk assessment phase. Information security policies and procedures are the foundation of Information Security effectiveness. Standards and procedures, decisions should be based on these policies. These policies help to prevent inconsistency and reduce security holes which can be exploited easily.

According to our approach there should be a framework which forms a basis for information security policy. This framework is used to develop organizational policies and procedures. There can be a policy repository which consists of sample polices. Policies stored in this repository can be used as is or can be revised. Organizations using this framework can administrate their policies and procedures.

3.6 Monitoring

Monitoring and reviewing the performance and effectiveness of the ISMS is part of the ISMS process. According to the ISO/IEC 27001:2005's Check phase organizations shall assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review [2].

Once certification is achieved, organizations should undergo periodic monitoring audits and must reapply for certification every three years. It is important that organizations use a governing system to automate the ISO/IEC 27001:2005

compliance and certification process, given the documentation and accountability requirements.

According to our approach organizations should review the security controls' implementation level and review the levels of residual risks and acceptable risks. They should conduct internal ISMS audits at planned intervals to review the level of implementation of the control objectives, controls, processes and procedures of their ISMS. They should also keep the historical data of security incidents and manage security incident and create reports by using these data.

Monitoring security controls helps to identify potential security-related problems in the ISMS that are not identified during the risk analysis.

Incident management is important especially to keep the historical data of security incidents. By using these data incident statistics can be generated. Incident statistics are valuable in determining the effectiveness of security policies and procedures implementation. Incident statistics are used to assess security posture of organizations.

CHAPTER 4

IMPLEMENTATION

4.1 Introduction

In this chapter, the approach defined in Chapter 3 was implemented. It is a web based implementation in order to provide remote access for users without additional requirements. The implemented software is hosted on a web server so that users take the advantage of the software irrespective of time and place by only having access to internet. The proposed system ensures remote management of admin functions for Research Module.

Visual Studio .NET 2003 environment is used for software development and C# language is chosen. Microsoft SQL Server was selected for database implementation.

General description, database design and software design of the proposed system are explained in detail in the following sections.

4.2 General Description

As it is seen from Figure 4, this thesis has two main separated functions. First one is the tool named as InfoSec Toolkit which helps organizations by automating the process of the Information Security Management. The other one is Research Module which aims to take the picture of Information Security levels of organizations. In order to do so, one of the sub modules, Initial Gap Analysis Module is used. It not only includes an evaluation methodology but also includes a report generation system which uses historical data for reports to indicate comparative situation of different organizations either in a specified scope of business or a specified sector. In addition, a report, which takes the picture of current situation about Information Security and gives advices in order to strengthen the foibles of the organization, can be generated for a particular organization.

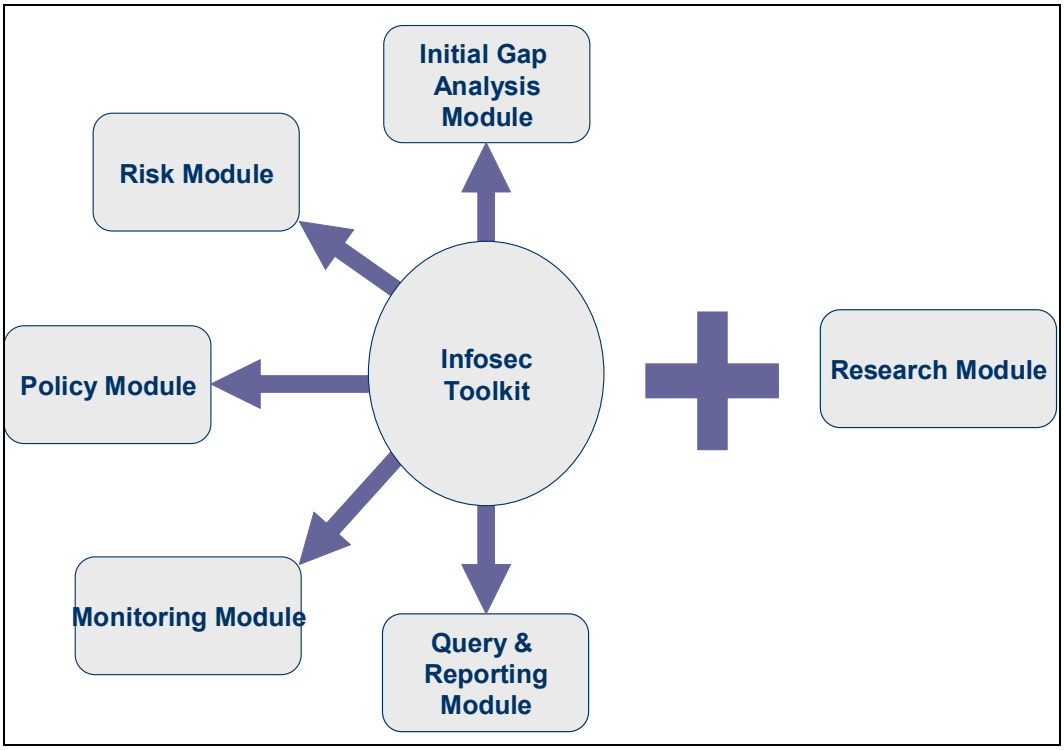


Figure 4 – General Description of the Thesis

InfoSec Toolkit is developed with five modules:

Initial Gap Analysis Module: This module consists of two sub modules. These are ISO/IEC 27001 Gap Analysis and Information Security Management System (ISMS) Gap Analysis. Initial Gap Analysis Module is used for identifying the current situation of the organization about Information Security and about ISMS if the organization has decided to be certificated.

Risk Module: This module is the key module of the overall system. This module is used to identify the organizations' information security scope, information assets, security requirements, threats, vulnerabilities, risks. These activities form the risk assessment process. After the risk assessment process organizations select controls from the pre-defined controls repository or create their own controls in order to mitigate the risks to an acceptable level.

Policy Management Module: This module has been constructed as an aid to organizations wishing to put in place a basic information security policy framework. It can be used to develop organizational policies. It has a policy repository which consists of pre-defined policies. Organizations can use the policy statements in the repository as it is or they can tailor them and store them in this repository. In addition organizations can attach pre-defined procedures to the related policies as required in all sorts of formats in order to define the implementation details of selected controls.

Monitoring Module: From the beginning to this point, the proposed system helps organizations to define and create an Information Security Management System. After this point organizations can use Monitoring Module to review and monitor the established system whether it is working properly or not. This module has three sub modules. These are Internal Audit Module, Control and Risk Review Module and Incident Management Module. Internal Audit Module uses Initial Gap Analysis' sub modules, namely ISO/IEC 27001 Gap Analysis and ISMS Gap

Analysis and the results can be reviewed comparatively. In Control and Risk Review Module organizations can create review sessions in order to review of the security controls' implementation level and review the levels of residual risks and acceptable risks. Incident Management Module has been constructed as a means of recording and managing the security incidents.

Query and Reporting Module: Using this module, organizations can make queries for their assets, threats, vulnerabilities, risks, selected controls and non-selected controls. And they can make queries for incidents entered in the incident repository as yet. In addition, organizations can generate some required documentations such as information security scope, asset inventory, risk assessment report, risk treatment plan, Statement of Applicability etc. by using this module.

Research Module: This module is prepared as a framework so as to take the picture of organizations' information security posture in Turkey. It uses one of the sub modules of Initial Gap Analysis, ISO/IEC 27001 Gap Analysis. This module allows generating an individual report peculiar to a specific organization and also generating comparative report of the selected organizations.

4.3 Conceptual Design of Database

Relational model was used for database design [17]. MS SQL server was used to implement database design as database management system. Since this thesis consists of two different parts, the conceptual database designs for each are different from each other. E-R diagrams of Infosec Toolkit and of research framework are given in Figure 5 and Figure 6 below successively.

For Infosec Toolkit, entities and relationships between them can be seen from Figure 5. All of the relationships are in Boyce-Codd Normal Form. After the normalization of the relations, 25 tables are generated to manage the data of the system.

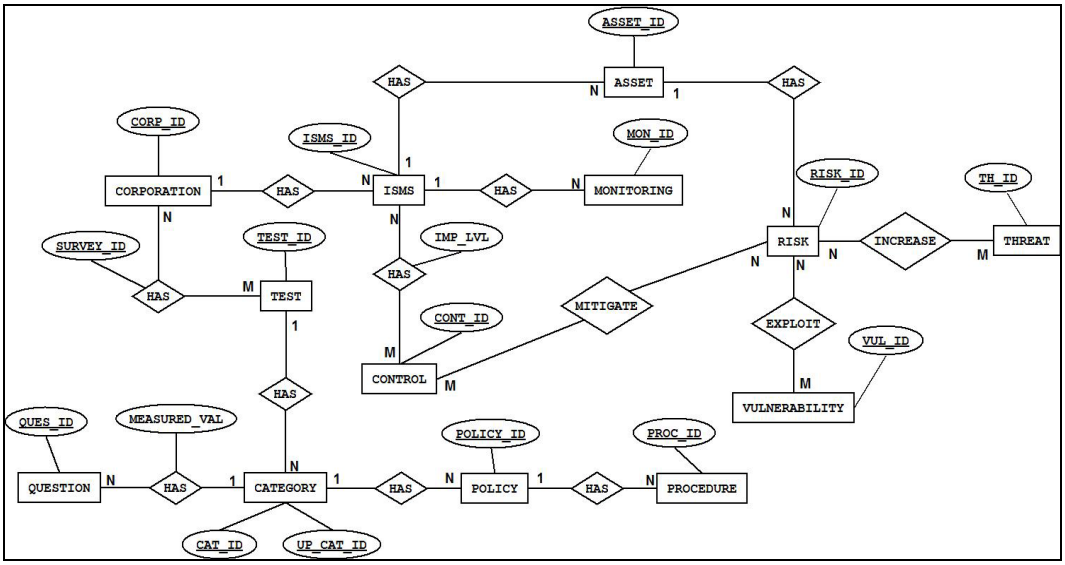


Figure 5 – E-R Diagram of Infosec Toolkit

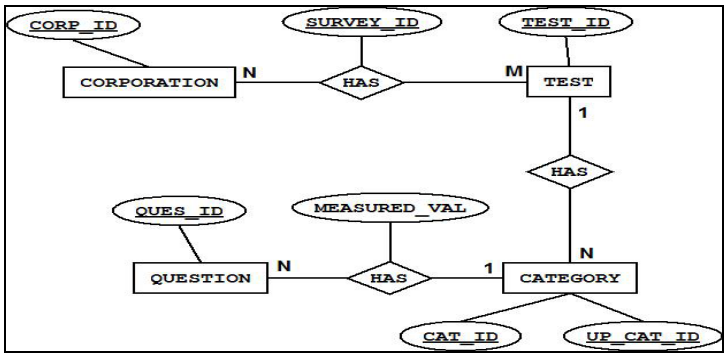


Figure 6 – E-R Diagram of Research Framework

For Research Framework, entities and relationships between them can be seen from Figure 6. All of the relationships are in Boyce-Codd Normal Form. After the normalization of the relations, 8 tables are generated to manage the data of the system.

4.4 Software Design

This section describes the software design for developing Infosec Toolkit and the research framework aimed to take the picture of Information Security levels of

organizations. These applications are developed to run on the Microsoft environment with .NET Framework Version 1.1, IIS V5.1 and MS SQL Server.

Object Oriented Programming Approach is used for the software design. UML Diagrams are drawn using Rational Rose Enterprise Edition. UML Diagrams and some required interface is in the following sections to explain the system clearly.

The said two modules are explained in the following sections in detail.

4.4.1 Infosec Toolkit

Use Case diagram of Infosec Toolkit for users is given in Figure 7. As it is seen from Figure 7, Infosec Toolkit has two user types; registered user and new user. There are totally ten use cases used for describing the system. These are Login, Fill Registration Form, Create/Choose ISMS Session, Initial Gap Analysis, Risk Module, Policy Management Module, Monitoring Module, Query and Reporting Module, Risk Management Module and Query Module. Create/Choose ISMS Session use case extends Fill Registration Form use case. Create/Choose ISMS Session is extended by Initial Gap Analysis, Risk Module, Policy Management Module, Monitoring Module, Query and Reporting Module. And lastly Risk Module is extended by Risk Management Module and Query Module. All these use cases are explained below in detail by the help of activity diagrams.

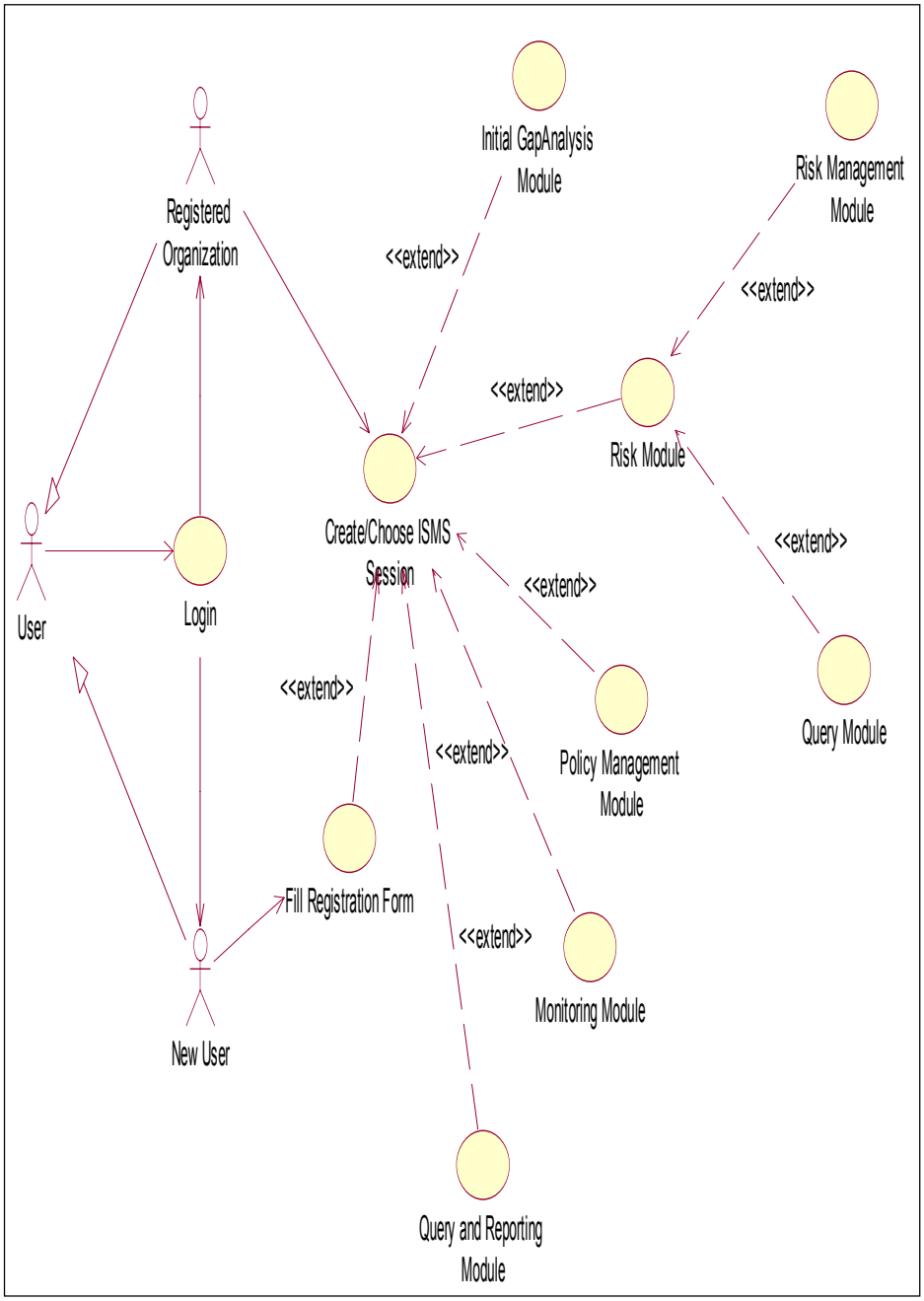


Figure 7 – Use Case Diagram of the Infosec Toolkit for Users

4.4.1.1 Login

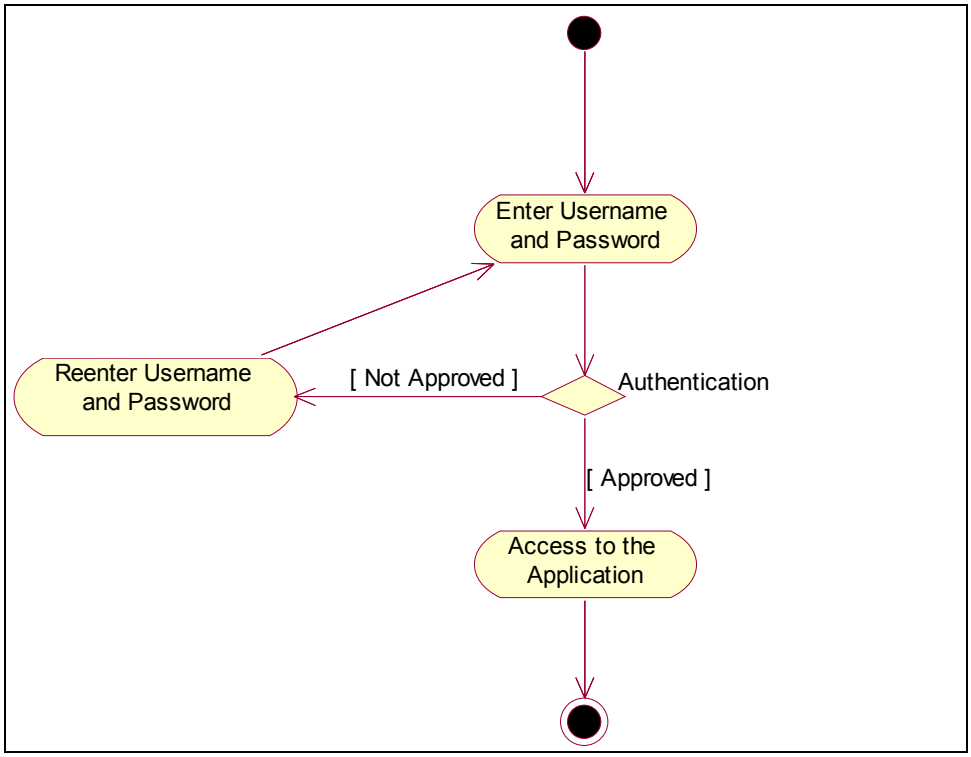


Figure 8 – Login Activity Diagram

User enters the application through this page. As it is seen from Figure 8 user enters username and password. Authentication level of user is determined during login and related functionalities are presented.

After entering the application by using his/her username and password, in order to use the application user should be registered to the system. Namely there are two kinds of user as shown in Figure 7; registered user and new user. If the user is a new one then user is redirected to the Fill Registration use case, or otherwise user is redirected to the Create/Choose ISMS Session.

4.4.1.2 Fill Registration Form

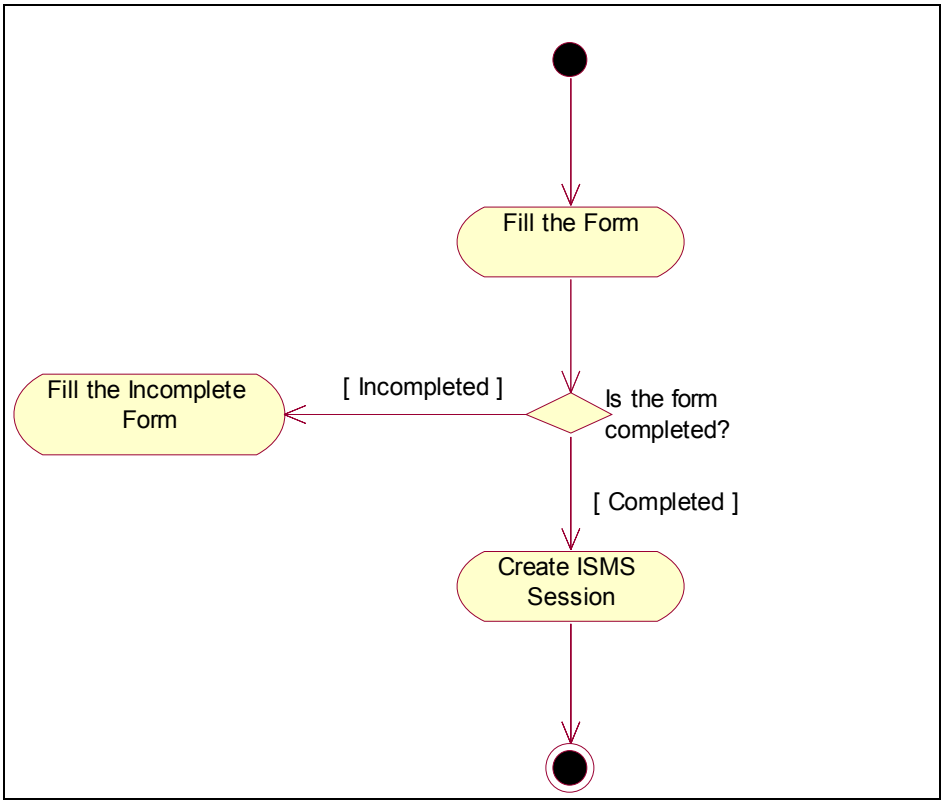


Figure 9 – Fill Registration Form Activity Diagram

Here user enters his/her personal information such as his/her name, surname, e-mail address, phone number and duty. He/she also enters organizational information such as name of the organization, where it is, the number of employee, business scope, sector, etc. and some information about the IT infrastructure of the organization. This information is used for reporting activities and is aimed to be used for the future work such as generating comparative reports on organizations using the information supplied here and other details generated during the usage of the tool. This form is filled only once.

4.4.1.3 Create/Choose ISMS Session

In this use case, user creates or chooses an ISMS session. If there is no existing session created previously, user should create a new session. If there is any session previously created, user can create a new session anyway or can choose a session from the session list. After selecting a session user can delete the selected ISMS, view the details of the ISMS or user can progress to the other modules.

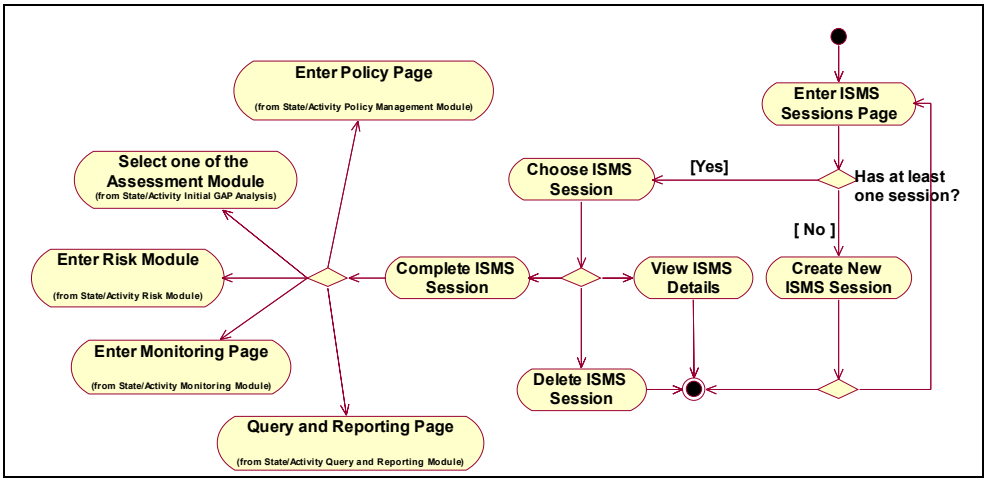


Figure 10 – Create/Choose ISMS Session Activity Diagram

4.4.1.4 Initial Gap Analysis

Reasonably, this module is the first module to be completed. Because before beginning establishing the ISMS, to decide the initial position of his/her organizations about information security is more sensible.

In this module there are two sub assessment modules. These are ISO/IEC 27001 Gap Analysis and Information Security Management System (ISMS) Gap Analysis. Firstly user selects one of the sub modules to complete. If the selected assessment has been completed already, user is directed to the report page on which user can view results of the assessment as a chart. A sample report can be

seen in Figure 12 below. If the selected assessment has not been completed yet, after selecting a category user continues answering the questions related with the selected category. Each assessment booklet has different number of categories and questions. ISO/IEC 27001 Gap Analysis has 11 categories and totally accumulated 133 questions. Information Security Management System (ISMS) Gap Analysis has 6 categories and 81 questions. The results of the assessments are stored on a database for future comparisons with the assessment results of internal audits. While user is answering the question, he/she defines the justification and reasons of his/her answer.

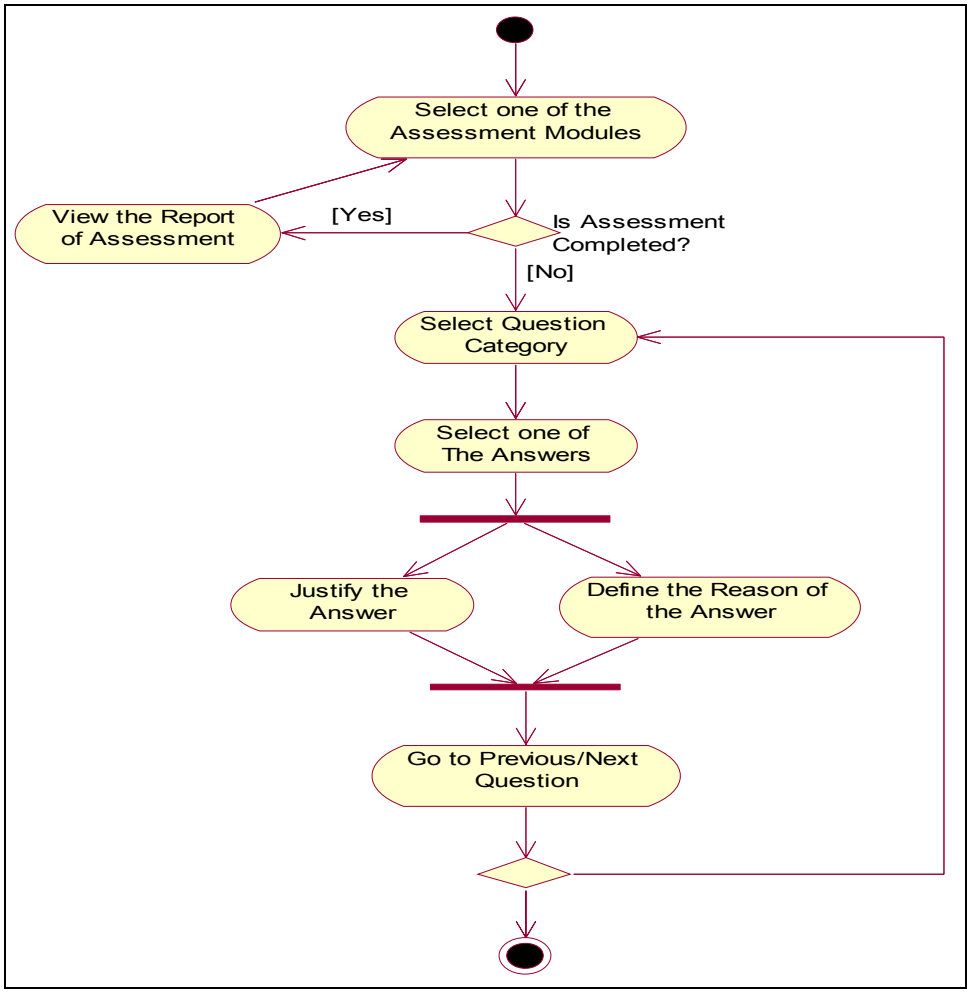


Figure 11 – Initial Gap Analysis Activity Diagram

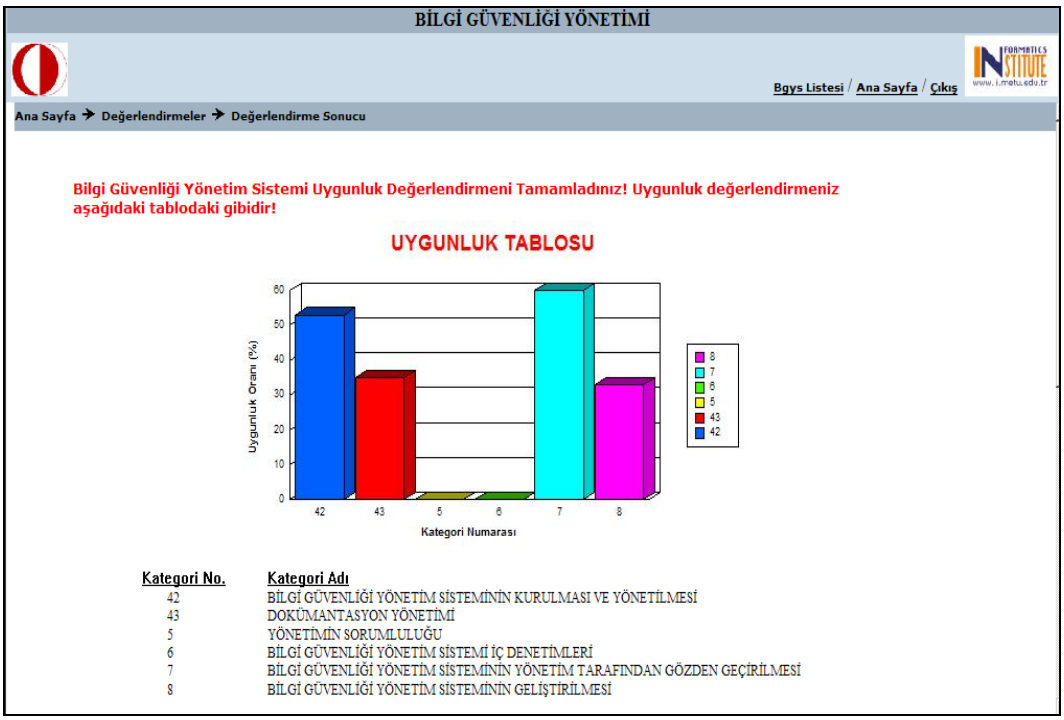


Figure 12 – A sample report which generated by Initial Gap Analysis Module

4.4.1.5 Risk Module

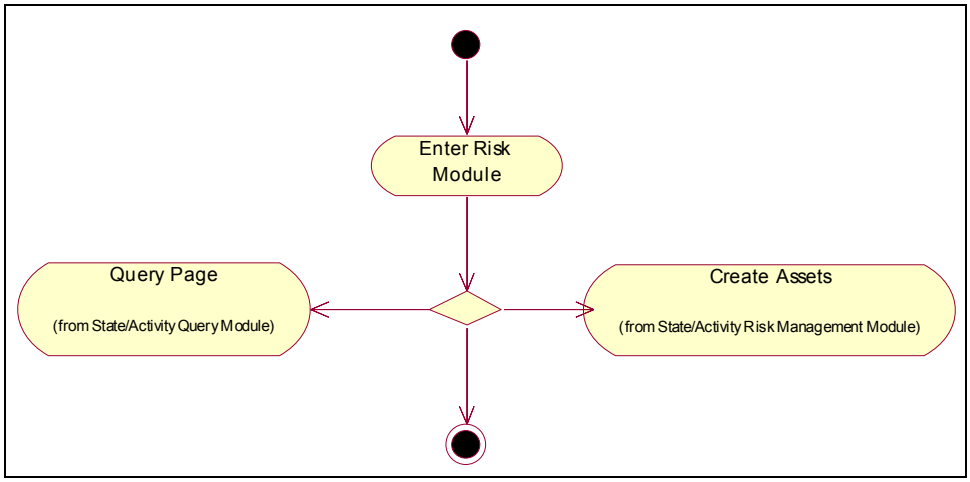


Figure 13 – Risk Module Activity Diagram

This use case is an entry point of risk management processes. User can either go to the Query Module which is used for making queries, or go to the Risk Management Module. In fact there is no need to separate these two activities. Since there are too many activities under the Risk Module, it is better to divide it into two sub modules as Query Module and Risk Management Module for the sake of clarity.

4.4.1.6 Risk Management Module

User performs most of the ISMS establishment works in this module. As it is seen from the Risk Management Module Activity Diagram given in Figure 14, these establishment activities are; creating the organization's asset inventory, identifying security requirement, valuation of assets, identification of threats and vulnerabilities, defining ISMS risks, deciding risk treatment options, selecting security controls in order to mitigate risks for which "Select appropriate controls for reduce the risk" option is selected, deciding the reduced levels of risks, preparing implementation plan for selected controls and justifying the controls not selected why these are excluded.

At first for each ISMS a list of assets are given by default. These assets are the most common ones. These are categorized as information assets, software assets, physical assets, human resources and prestige assets [5]. User can use this asset structure as is or can modify to fulfill organization's need. User can create new categories and assets. User can choose assets from the asset list and then modify or can create from the scratch. And also user can delete assets or categories. Here also for each asset, description of asset, owner of it, e-mail address of the owner and identifier of the asset are defined. The interface of creating the organization's asset inventory is given in Figure 15 below.

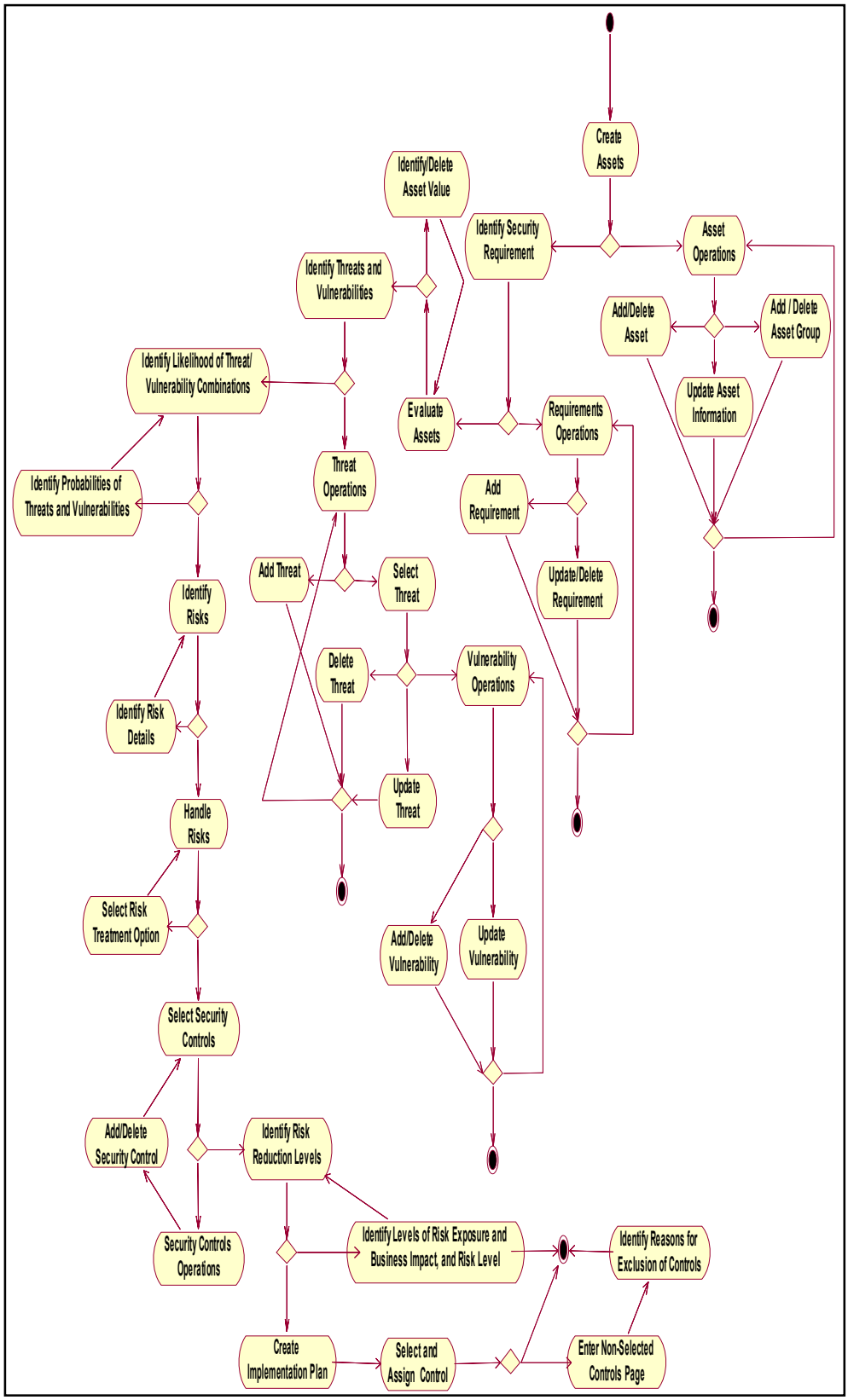


Figure 14 –Risk Management Module Activity Diagram

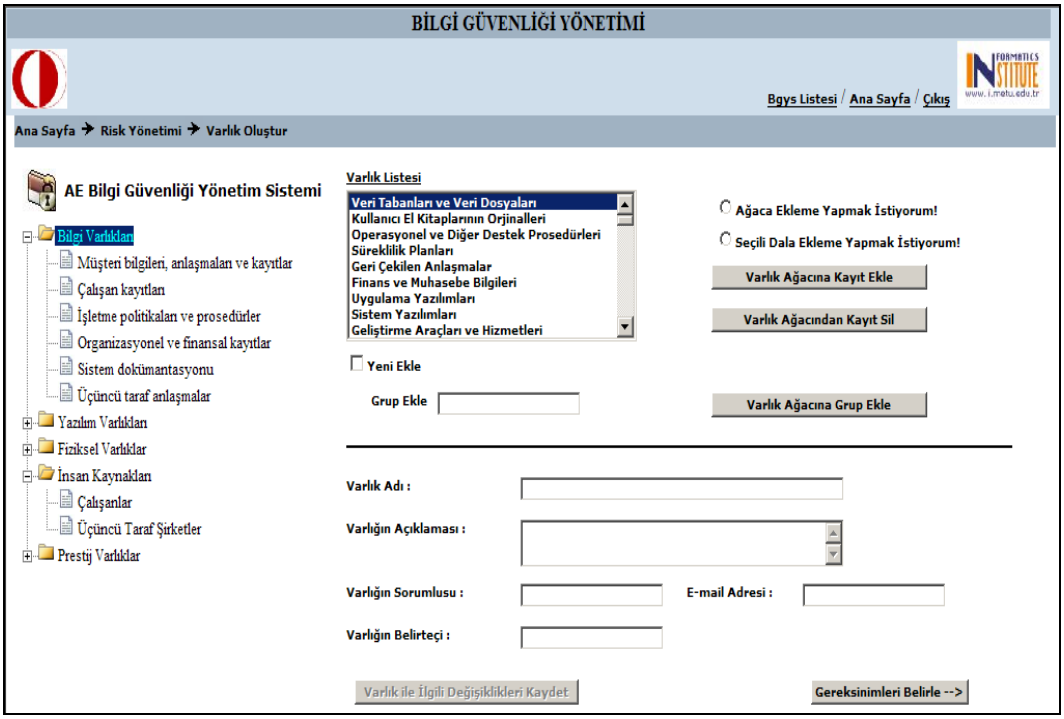


Figure 15 – Creating the Organization's Asset Inventory Interface

Next step is identifying security requirements. After creating asset inventory, for each asset user define security requirements and short description of them. There is repository which stores security requirement samples and every security requirement different from the requirements listed in the list is stored also in the repository. User can select from this repository or can create on him/her own. User can also delete requirements.

And then user evaluates the assets created in the related phase. Every asset is evaluated according to the loss of confidentiality, integrity and availability. In some cases these three criteria are not sufficient alone. In such cases an additional criterion can be introduced to meet these requirements. The interface of asset valuation is seen from Figure 16.

Identification of threats and vulnerabilities is the part of identifying security requirements. Here user defines the threats and vulnerabilities related with the

selected asset. Using this interface, user can define threats and vulnerabilities by selecting pre-defined threats and vulnerabilities or by creating from the scratch. User also deletes and updates the selected threats or vulnerabilities. Here again there are threat and vulnerability repositories which helps the user during identification of threats and vulnerabilities.

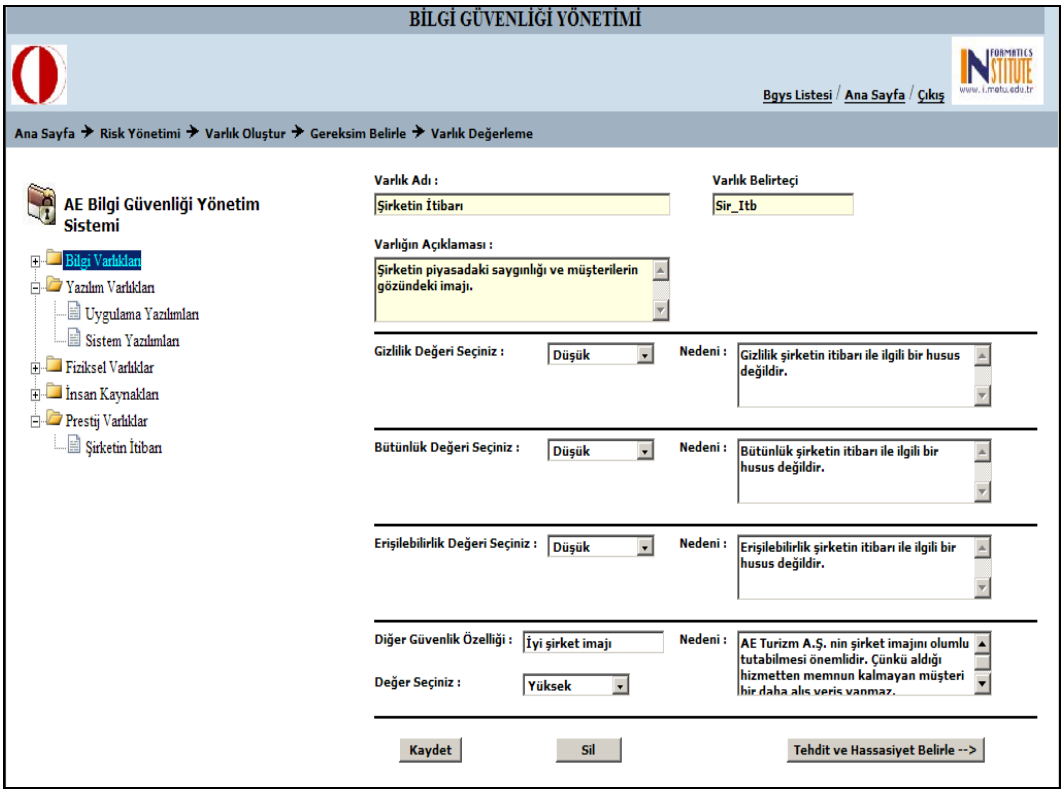


Figure 16 –Identifying security requirements

In the next phase, user determines the likelihood of threat and vulnerability level for each threat-vulnerability combinations related with the selected asset. In addition user describes the threats and vulnerabilities, and explains the reasons of them. And lastly user identifies the security properties for selected threat-vulnerability combination. The interface of this phase is given in Figure 17.

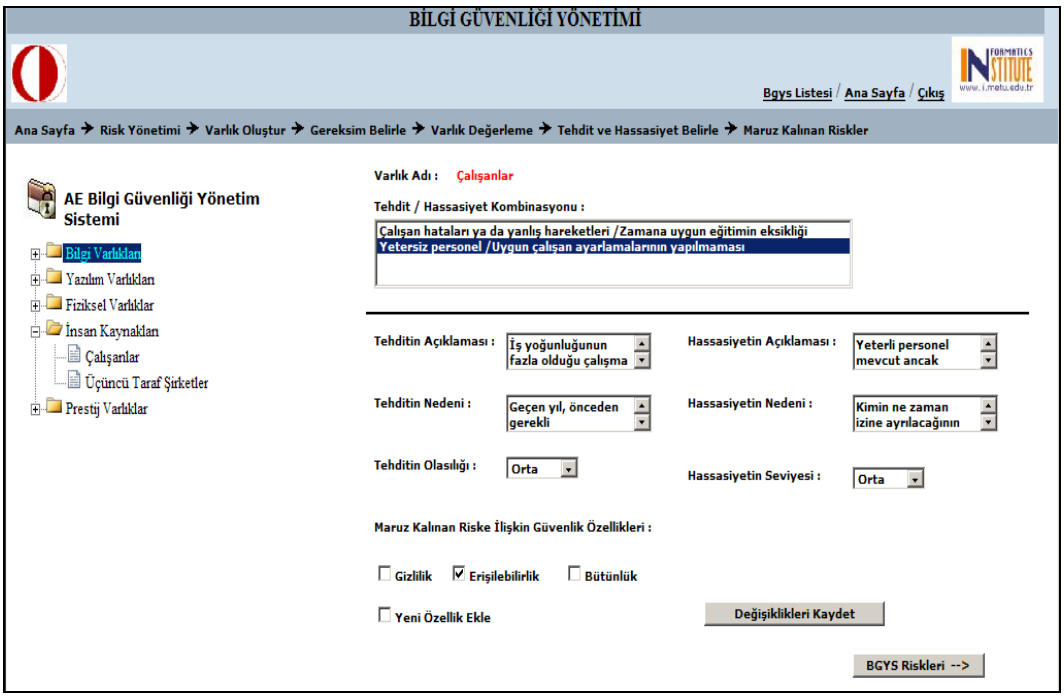


Figure 17 - Determining the likelihood of threat and vulnerability level

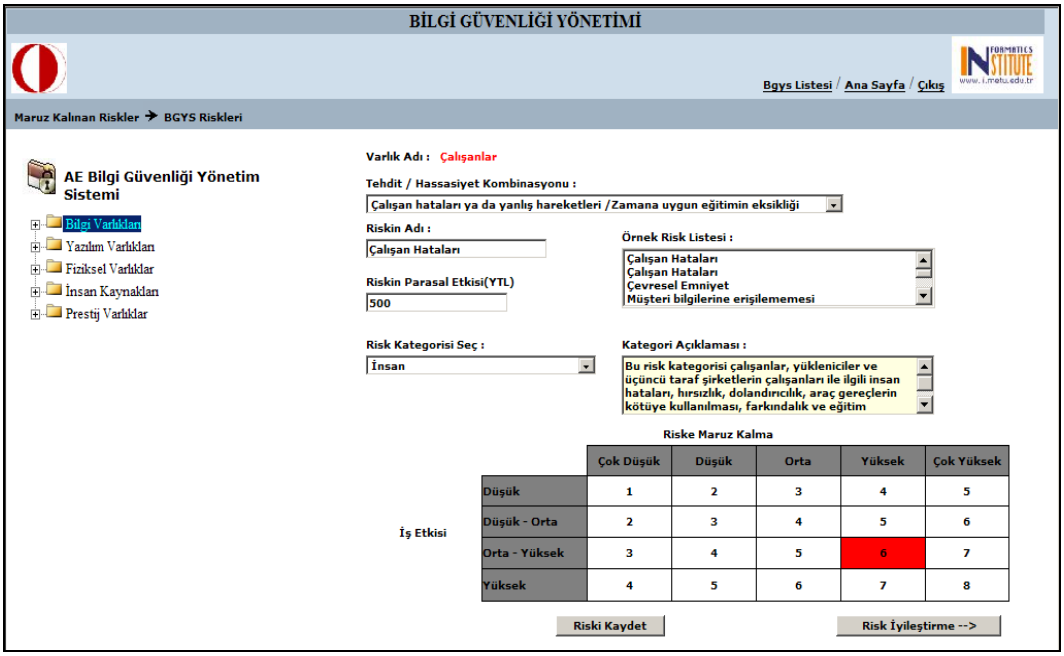


Figure 18 – ISMS Risks

And next, user defines the security risks. In fact each threat and vulnerability combination composes a risk. Here user gives a name for each risk, put it in a risk category and decide the monetary impact of the risk. Thereto user views the risk level from a chart. Risk level is calculated automatically as defined in section 3.4.1.5. The interface this phase is given in Figure 18.

Next phase is the deciding risk treatment options. Here user selects an option from risk treatment options described in section 3.4.2 and explains the rationale for this decision. The interface is seen from Figure 19.

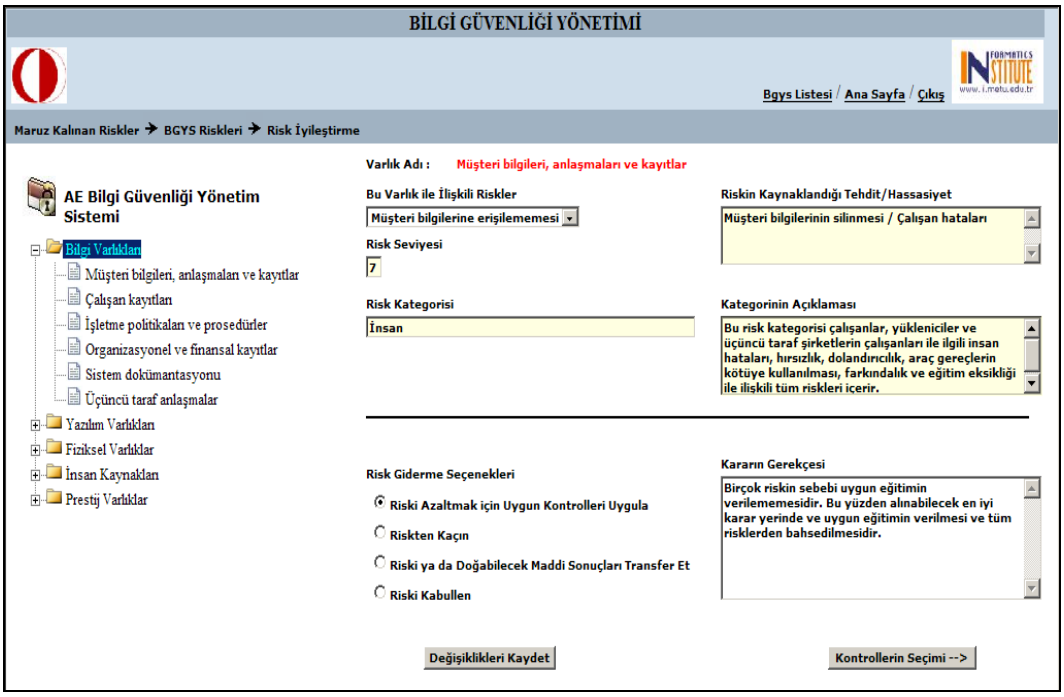


Figure 19 – Deciding risk treatment option

If the risk treatment decision is to mitigate the risk by implementing appropriate security controls, in the next phase user identifies controls to mitigate the selected risk. User can either add from pre-defined controls repository which stores for the time being only controls of ISO/IEC 17799:2005, or add or delete his/her own controls. The interface of this phase is given in Figure 20 below.

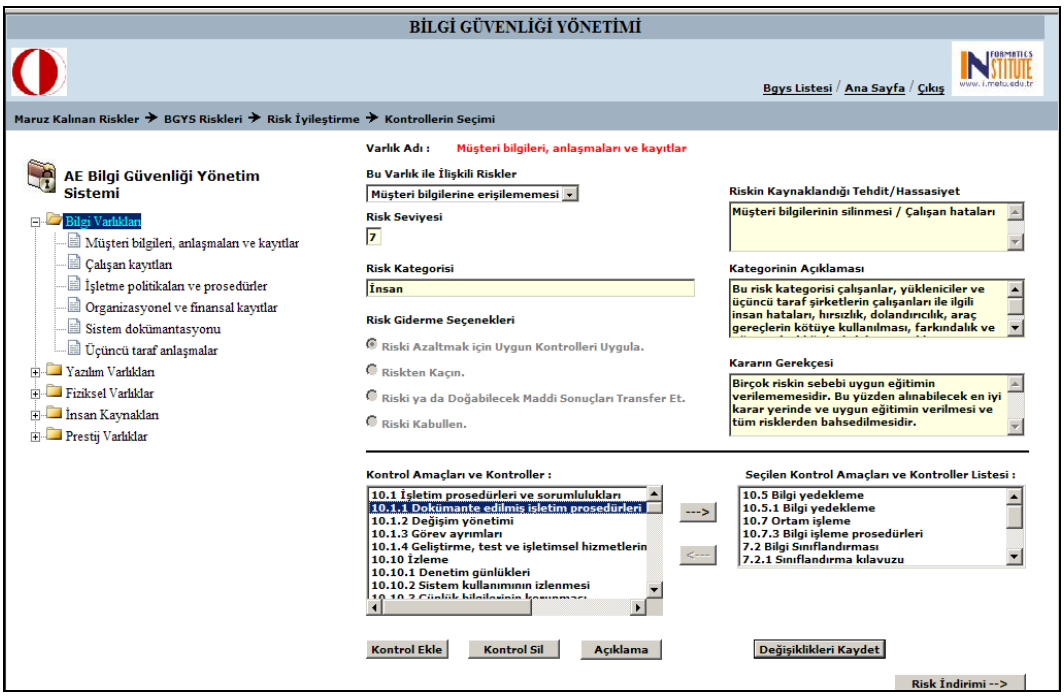


Figure 20 – Select security controls in order to mitigate risks

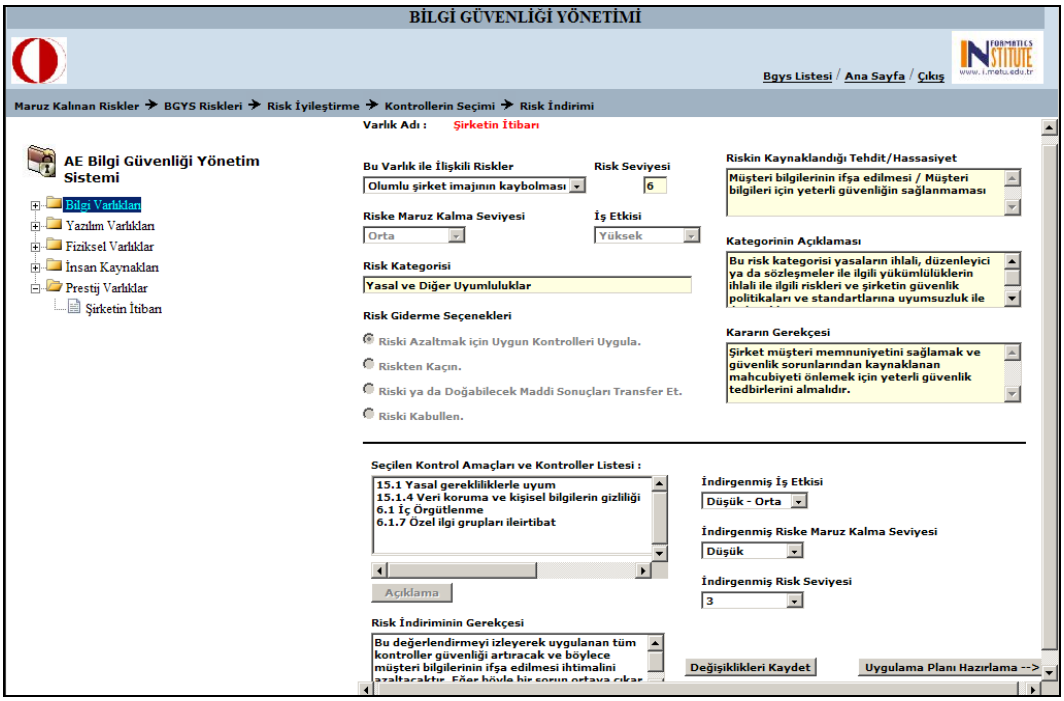


Figure 21 – Deciding reduced level of risks

After selecting security controls, user decides the reduced levels of risks and defines the rationale of the decision. The interface is seen from Figure 21.

By now all the assets, treats, vulnerabilities and risks are identified. Decisions about which security controls in the ISO/IEC 17799:2005 will be implemented are made in order to mitigate risks related with the assets. At this point user should create the implementation plan of selected controls and give the rationale for security controls which is not selected to mitigate the risks.

To create implementation plan for controls user uses the following interface and determine the responsible person, beginning and finish date of the implementation, implementation priority, resources for and cost of implementation.

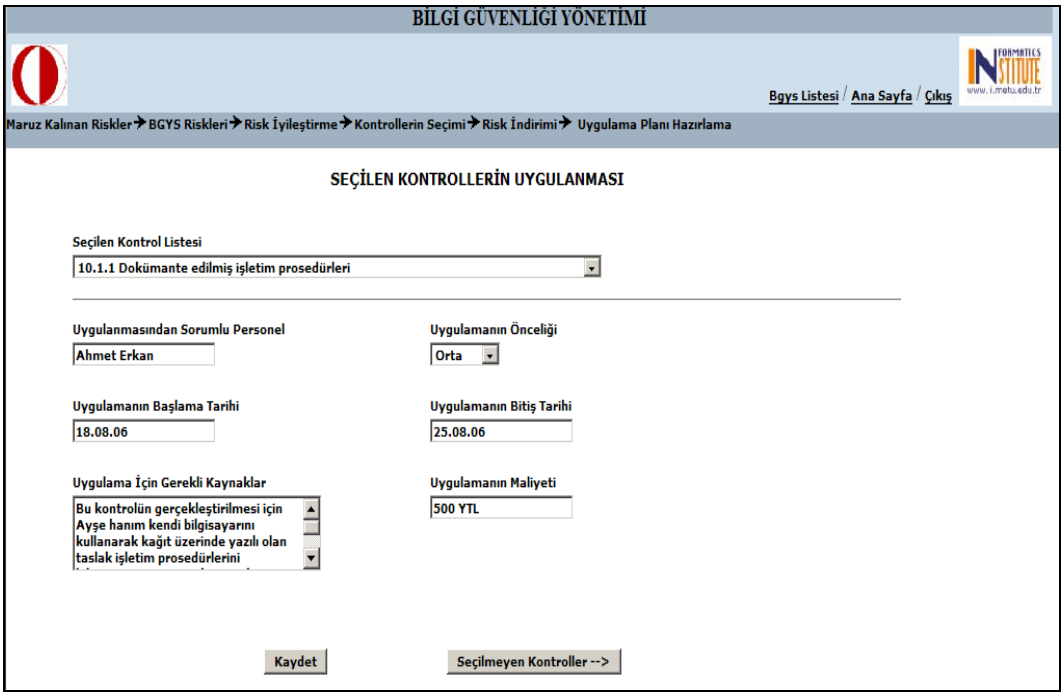


Figure 22 – Implementation plan for selected controls

And lastly, user states the rationales for security controls which will not used for mitigating risks.

4.4.1.7 Query Module

The other module extended from Risk Module is Query Module. User uses this module to make queries on information generated through the Risk Management Module. As seen from the Figure 23 below, user can make queries on assets, threats, vulnerabilities, security requirements, risks, selected controls and not selected controls. After defining the query criteria and selecting the items from the list on which query is made, user can view the results. Results is listed in tabular form and some of the information on the table has hyperlink which is used to go the related pages in order to change the listed information or just to view the details of the item according to the selected item. An example of query results page is given in Figure 23 below.

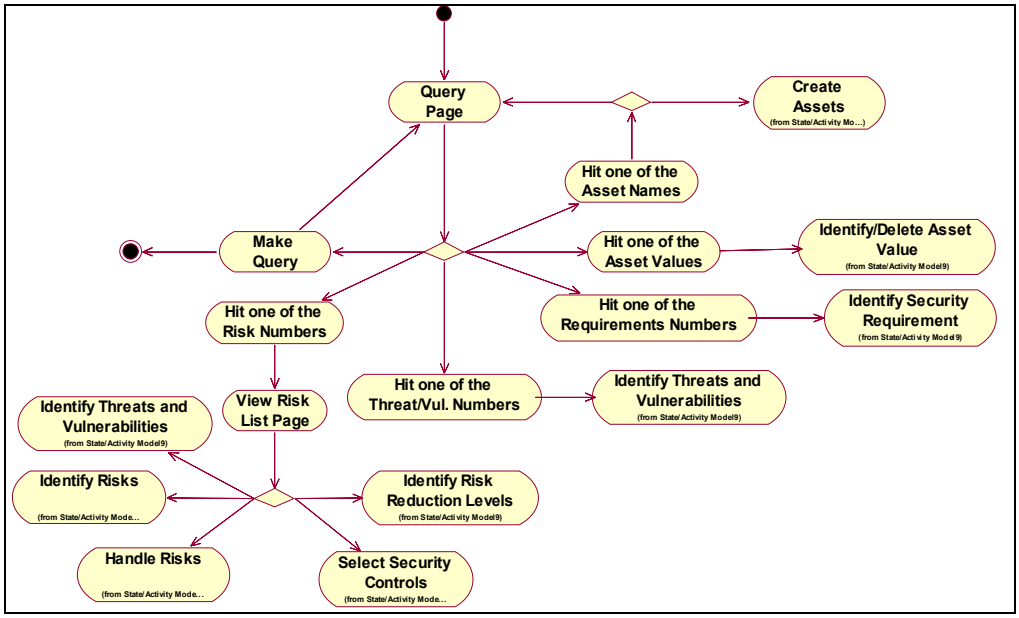


Figure 23 – Query Module Activity Diagram

As it is seen from Figure 24, user can make queries on different groups of information. These are mentioned above. User selects the different criteria for each group and enters keyword for the query. According to the criteria results is shown in tabular form.

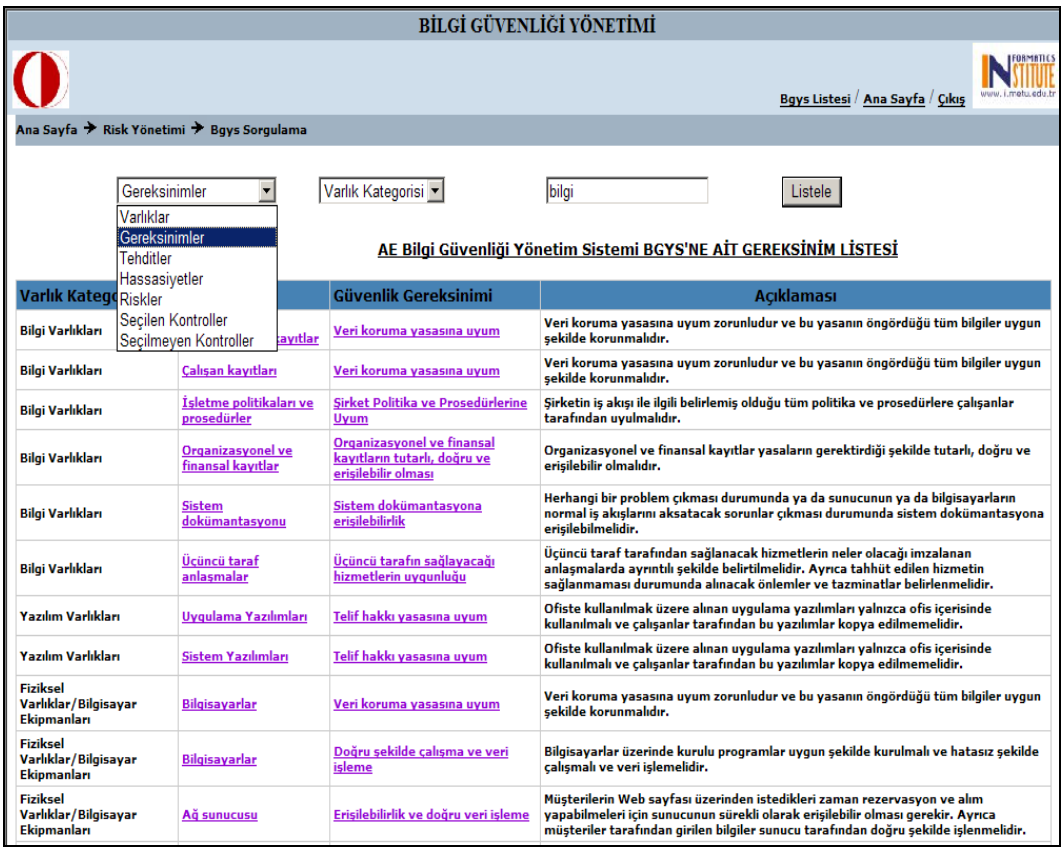


Figure 24 – An example of query results page

If the user hit one of the risk number links, user redirected to a page on which details of this information is shown. This page's interface is given Figure 25.

Using these links shown Figure 24 below, user can go to the related page in order to modify the information.

If the user hits one of the asset name links shown in Figure 24, user redirected to a page on which the details of the asset is shown. Figure 26 shows this page. From this page user can either go back to Query Module or go to the Risk Management Module's related page in order to modify the information.

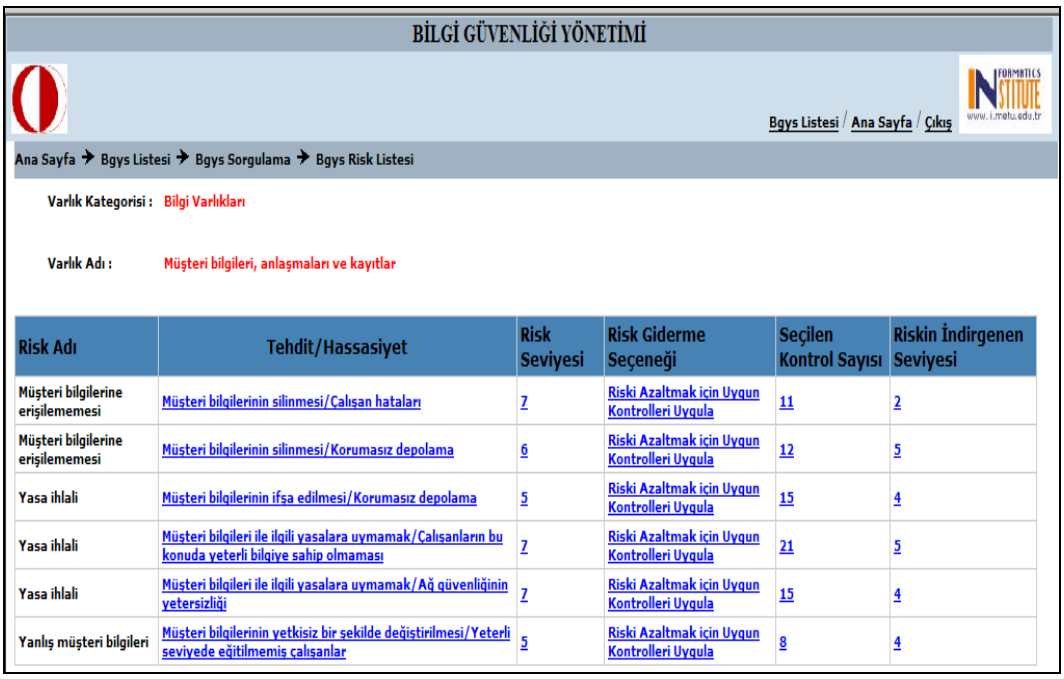


Figure 25 – Risk details page

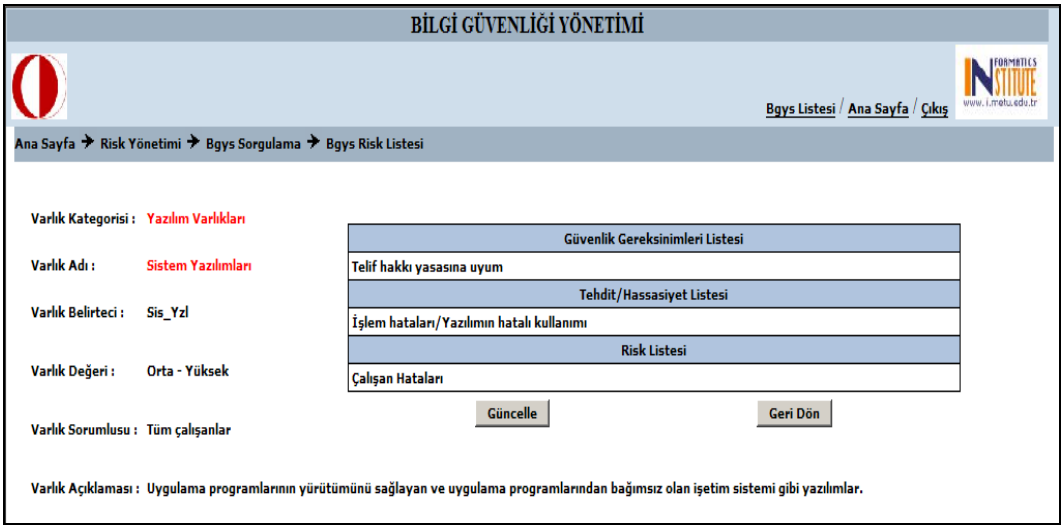


Figure 26 – The page on which details of selected asset are shown

4.4.1.8 Policy Management Module

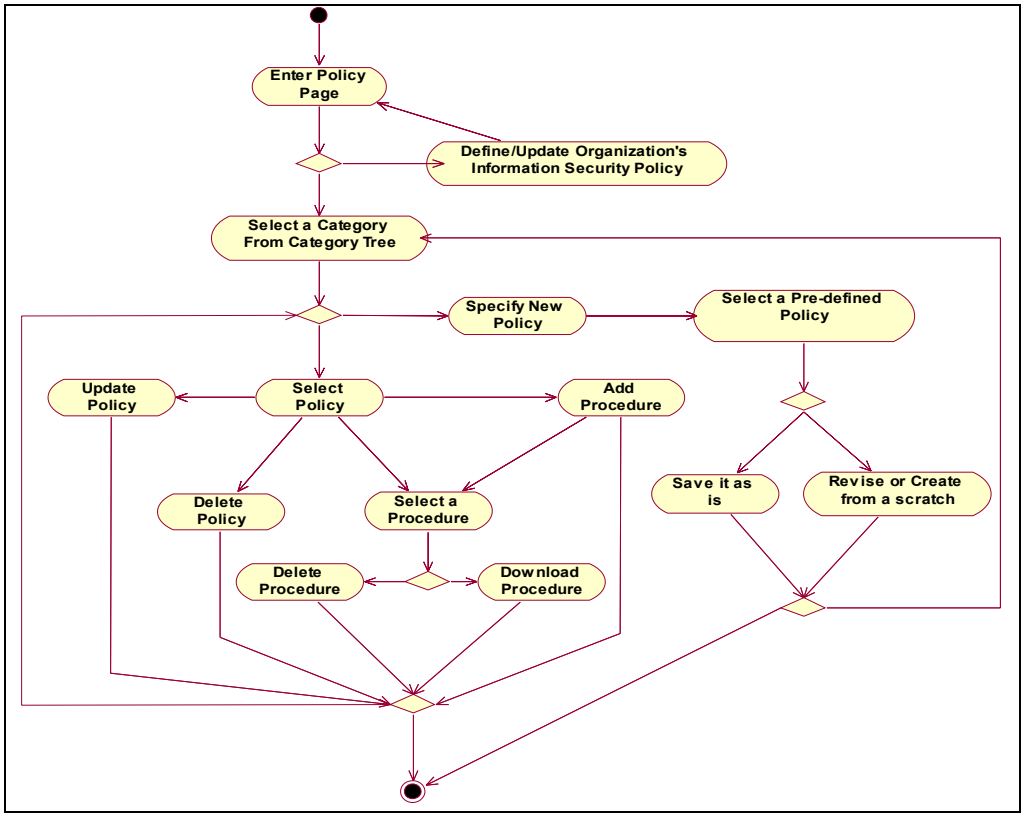


Figure 27 – Policy Management Module Activity Diagram

There is a policy repository which stores pre-defined policies. These policies are categorized in categories. These categories also have sub categories. There are 11 main categories and 39 sub categories totally accumulated under these 11 categories. These categories and sub categories are taken from ISO/IEC 27001:2005.

Before create the policy framework user defines his/her organization's information security policy. This policy document indicates the goals of information security.

To construct a policy framework for his/her organization in line with the organization's information security policy, after choosing a category or sub

category from category tree user specify a policy for the related category. User can specify a policy in two ways. He/she either create a new policy or select a pre-defined policy from the policy repository. The policy selected from the policy repository can be used as is or can be revised. User deletes or updates a policy after selecting from the policy list.

In order to attach a procedure to a policy, first of all user should select a policy and then select a pre-defined procedure in all sorts of formats. Procedures contain the implementation details of selected controls. User also after selecting a procedure attached beforehand, delete or download the procedure.

4.4.1.9 Monitoring Module

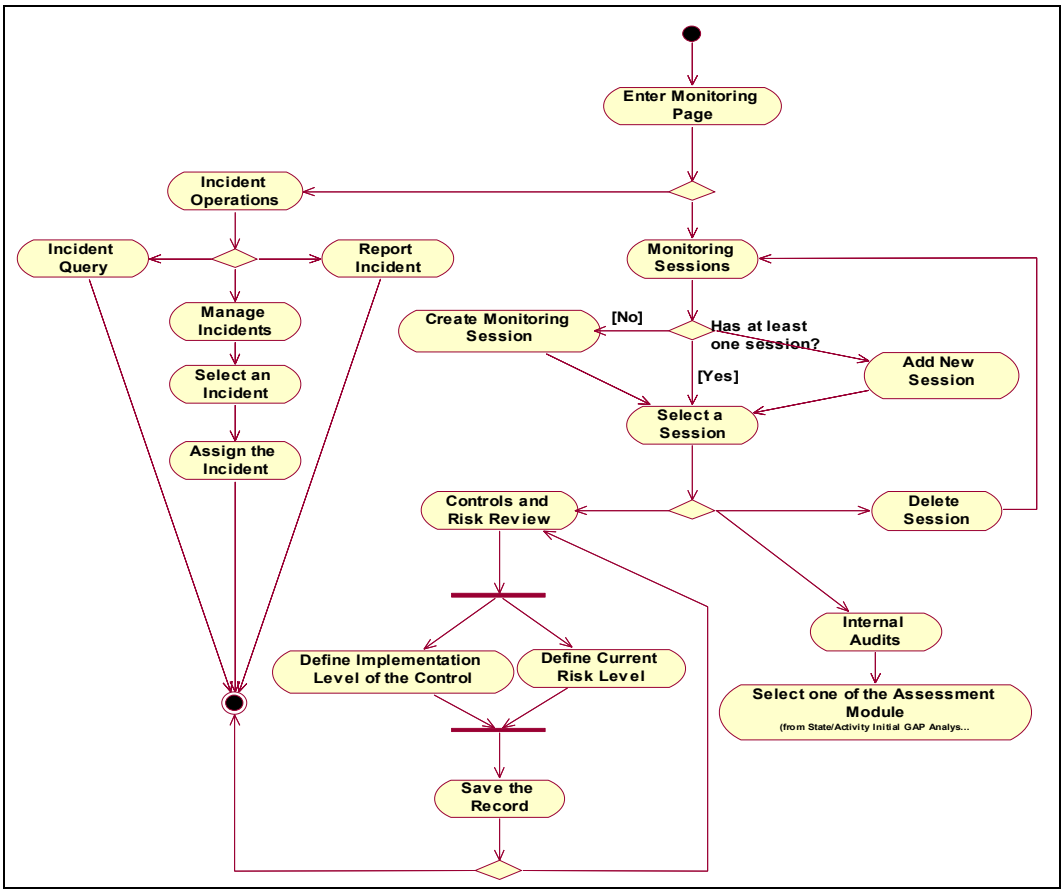


Figure 28 – Monitoring Module Activity Diagram

Monitoring module is one of the biggest distinctions from the other tools cited in this thesis. This module has three sub modules. These are incident management, internal audits and control and risk review. Internal audits and review of controls and risks are under Monitoring Operations. User should use these operations under a monitoring session. Without defining a session for these operations, information gathered from these sub modules can not be categorized or handled in order to review or monitor the status of ongoing activities. But on the other hand the incident operations are not performed under a monitoring session.

At first, user selects to go either incident management or monitoring sessions. In incident management module user can perform three functions. These are reporting incident, incident management and incident query. In order to report an incident, user fills a form having details of the incident. This form is shown in Figure 29.

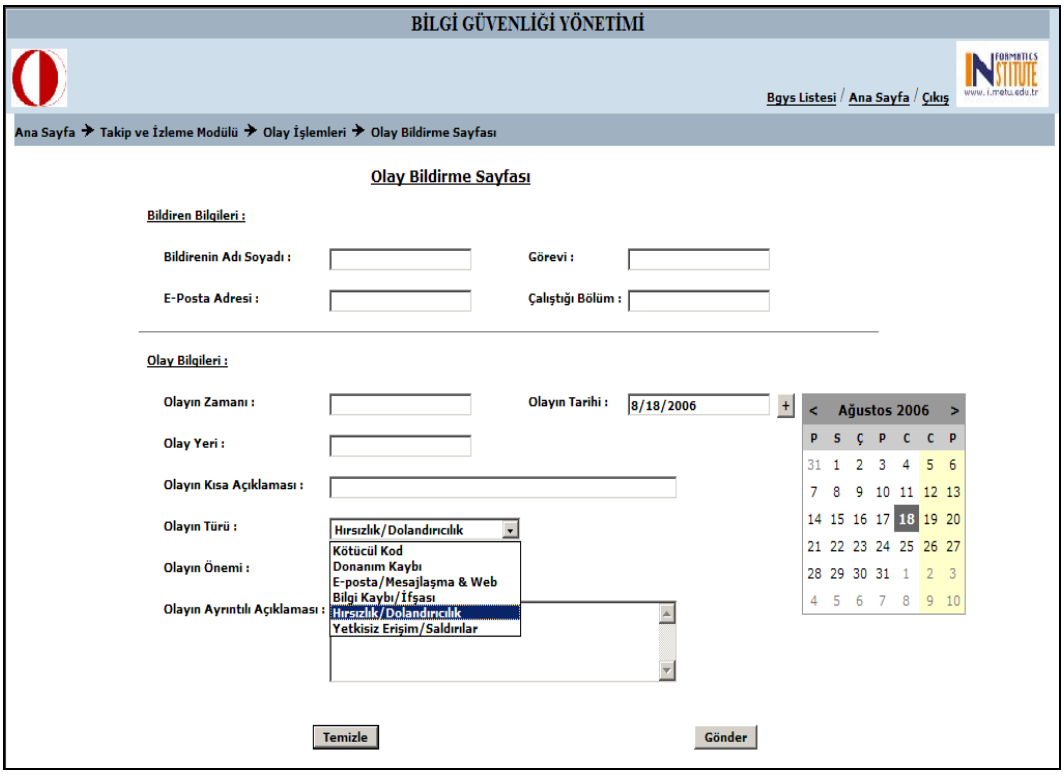


Figure 29 – Incident reporting form

In order to respond an incident, it is important to decide how serious it is. User defines the details of incident response information. User decides the seriousness of the incident at first and then defines type of the incident, due date of removing the incident's results, effects of the incident etc., what will be done and who will be responsible for the incident. Incident management page is given in Figure 30 below.

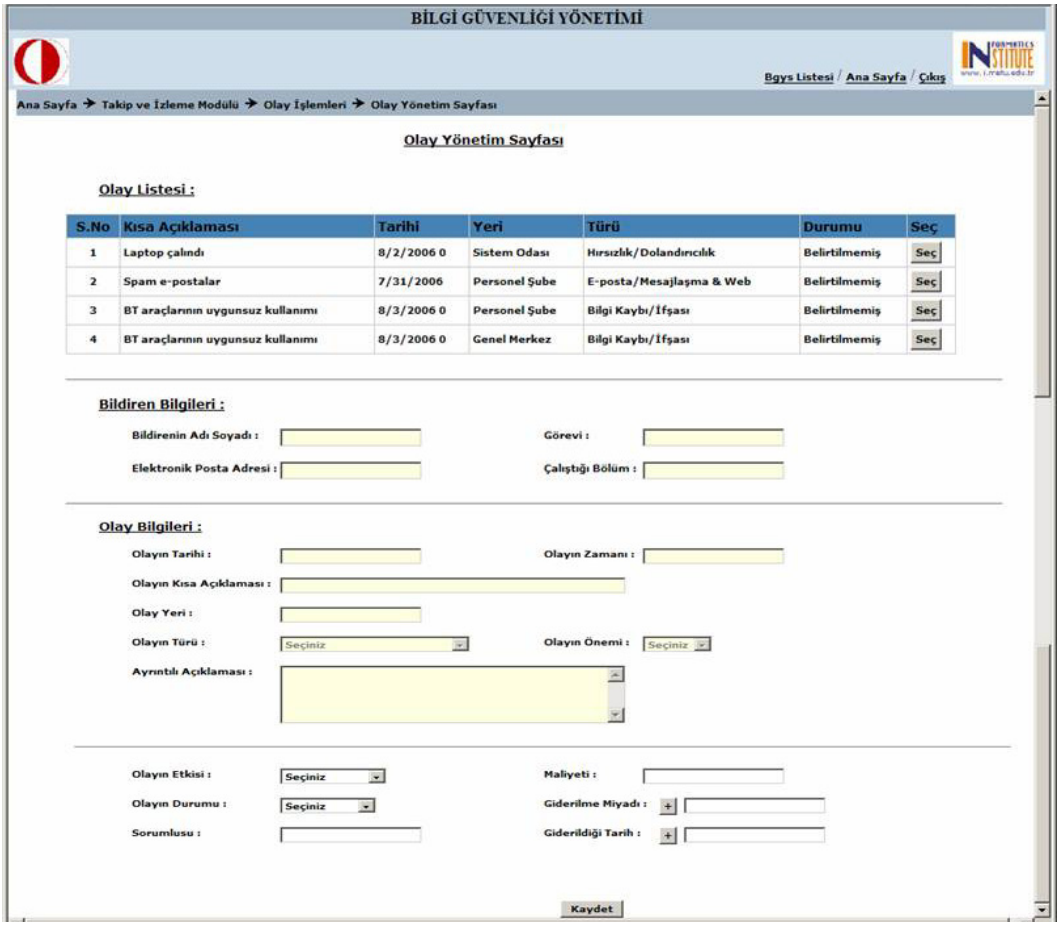


Figure 30 – Incident management page

4.4.1.10 Query and Reporting Module

Query and Reporting Module activity diagram is given in Figure 31. In this module user has three opportunities. These are ISMS Query, Incident Query and Reporting

on the ISMS. ISMS query uses the Query Module defined under Risk Module. Likewise Incident Query uses the query capabilities of Monitoring Module.

In Reporting on the ISMS, user can report on some information generated during ISMS processes. User can generate some required documents such as Organization's Information Security Policy, details of the ISMS, asset inventory, risk assessment report, risk treatment plan, Statement of Applicability. In addition, user can also view reports on the results of Internal Audits or Initial Gap Analyses after selecting an assessment from the assessment list.

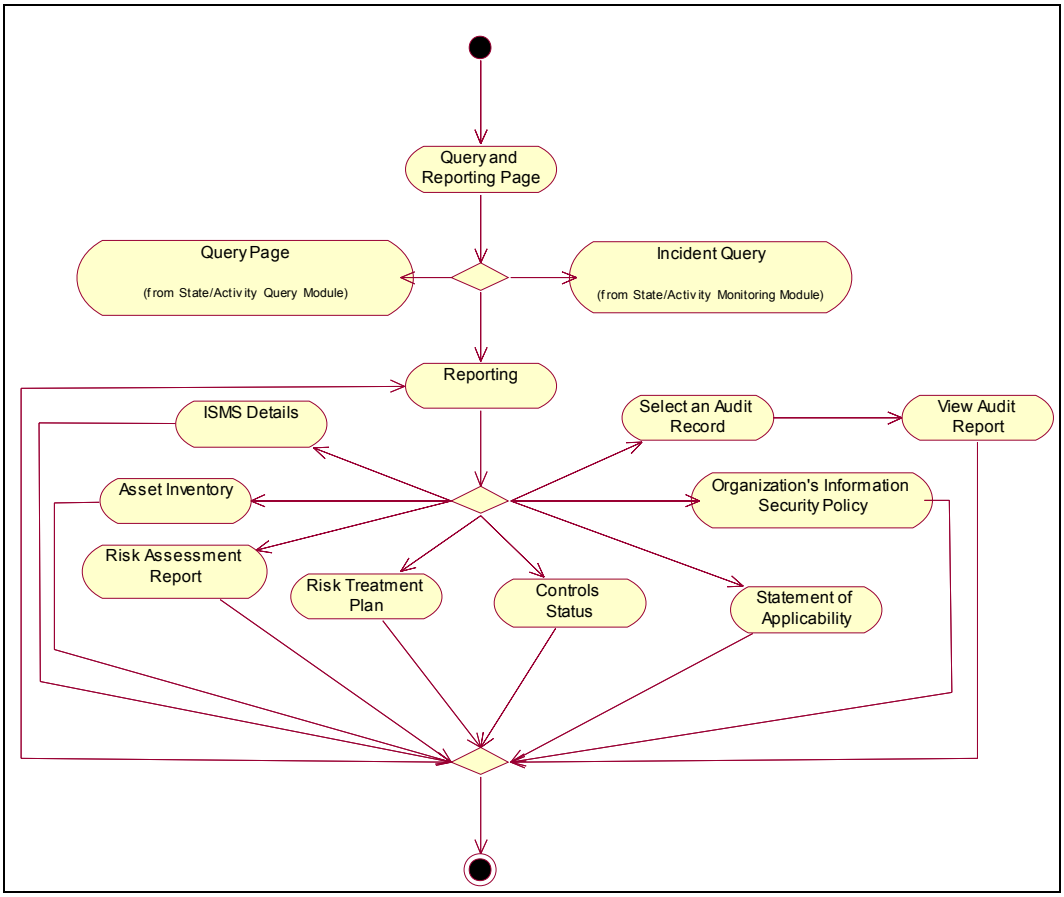


Figure 31 – Query and Reporting Module Activity Diagram

4.4.2 Research Module

Software design of the research framework is described in this section by the help of use case diagrams and interfaces. This module has two sub modules. One of the modules is used by administrators of the system, and the other one is used by the organizations which are participated in the research as users.

Admin Module is the first sub module of Research Module. Use Case diagram, on which the details of admin module are depicted, is given in Figure 32.

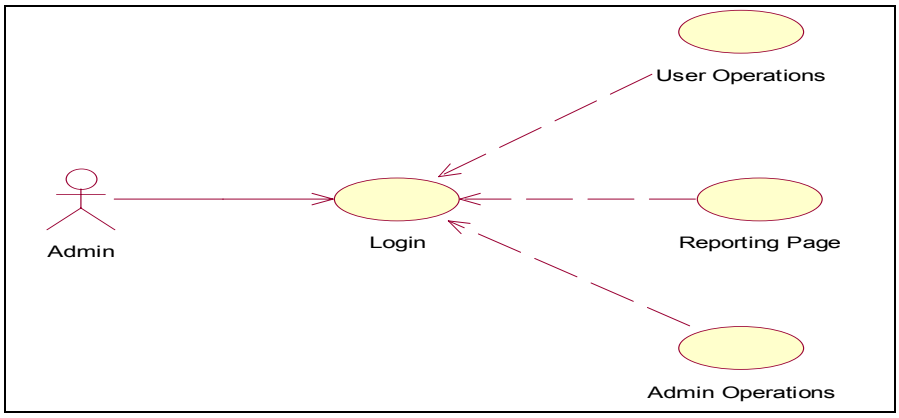


Figure 32 – Admin Module Use Case Diagram

As it is seen from Figure 32, after the admin logins the system, there are three main capabilities that the admin can perform. These capabilities are explained in the following section.

Login activity is the same as Login activity of Infosec Toolkit which is explained in section 4.4.1.1. Thus, details of this activity are not explained here.

Administrators can view and modify their user information by using Admin Operations sub module.

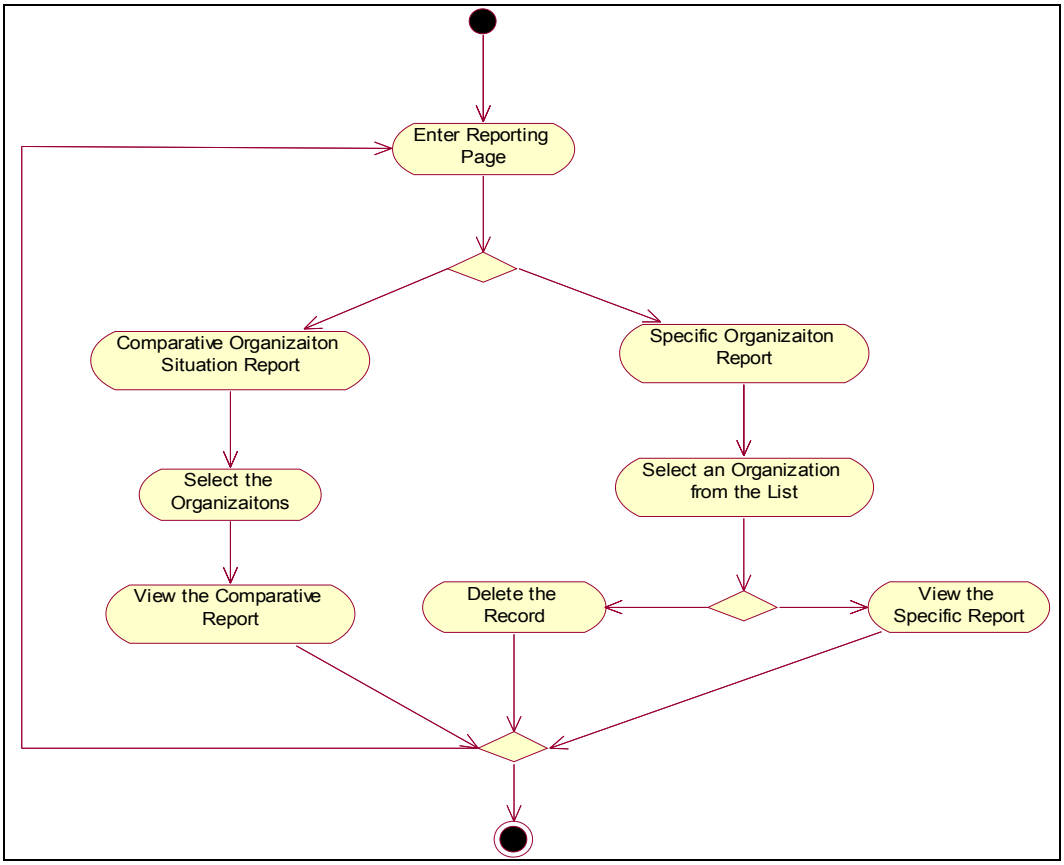


Figure 33 – Reporting Page Activity Diagram

Reporting Page activity diagram is given in Figure 32 above. As it is seen from the Figure 32, there are two different reporting capabilities in Admin Module. Administrator can either generate comparative report which compares the selected organizations' information security situations or specific reports about a specific organization.

And the last sub module of Admin Module is User Operations. Administrators can add a new organization, and after selecting an organization from the list can either delete or modify the selected organization's information. The activity diagram of this module is given in Figure 34.

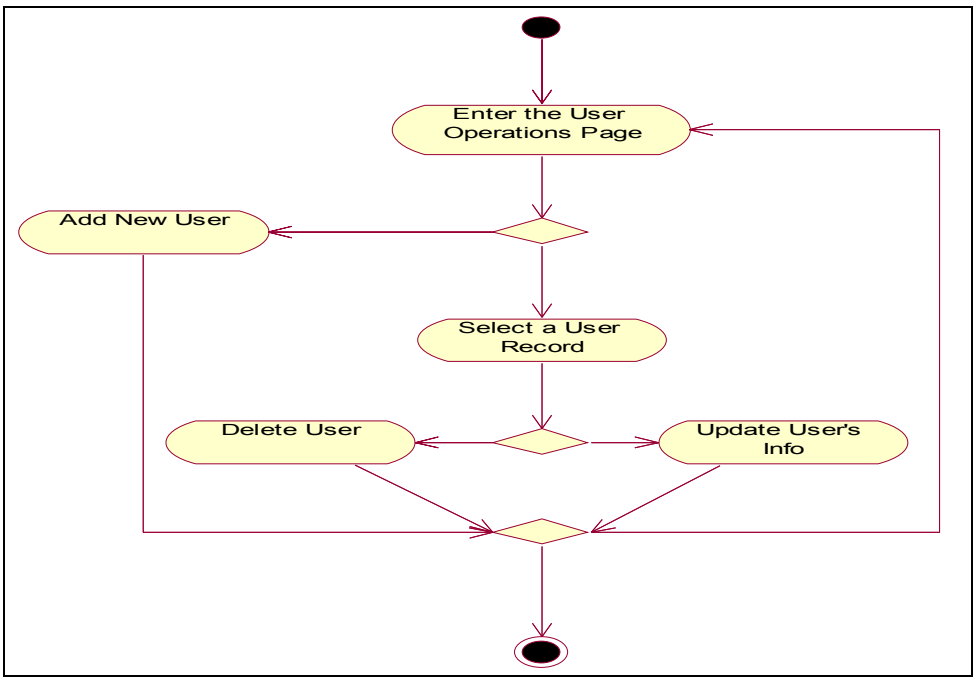


Figure 34 – User Operations Activity Diagram

The other sub module of Research Module is User Module. Use Case diagram of User Module is given in Figure 35.

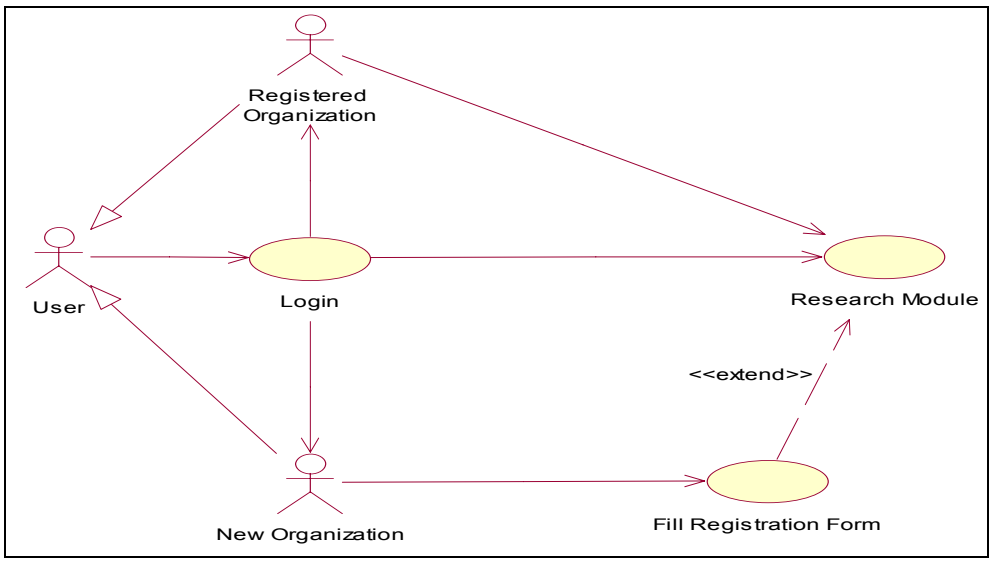


Figure 35 – Use Case Diagram of User Module

After created an account for an organization by administrator, the organization enters Research Module. If the organization has not filled the registration form, the organization is redirected to the registration page. Information supplied with this form is used for reports. After the organization fills the registration form, user accesses the assessment page. In Research Module, one of the sub assessment modules of Initial Gap Analysis Module, ISO/IEC 27001 Gap Analysis, is used. The details of this module are explained in section 4.4.1.4. Activity diagram of this module depicted in Figure 36 is a little bit different from the ISO/IEC 27001 Gap Analysis activity diagram.

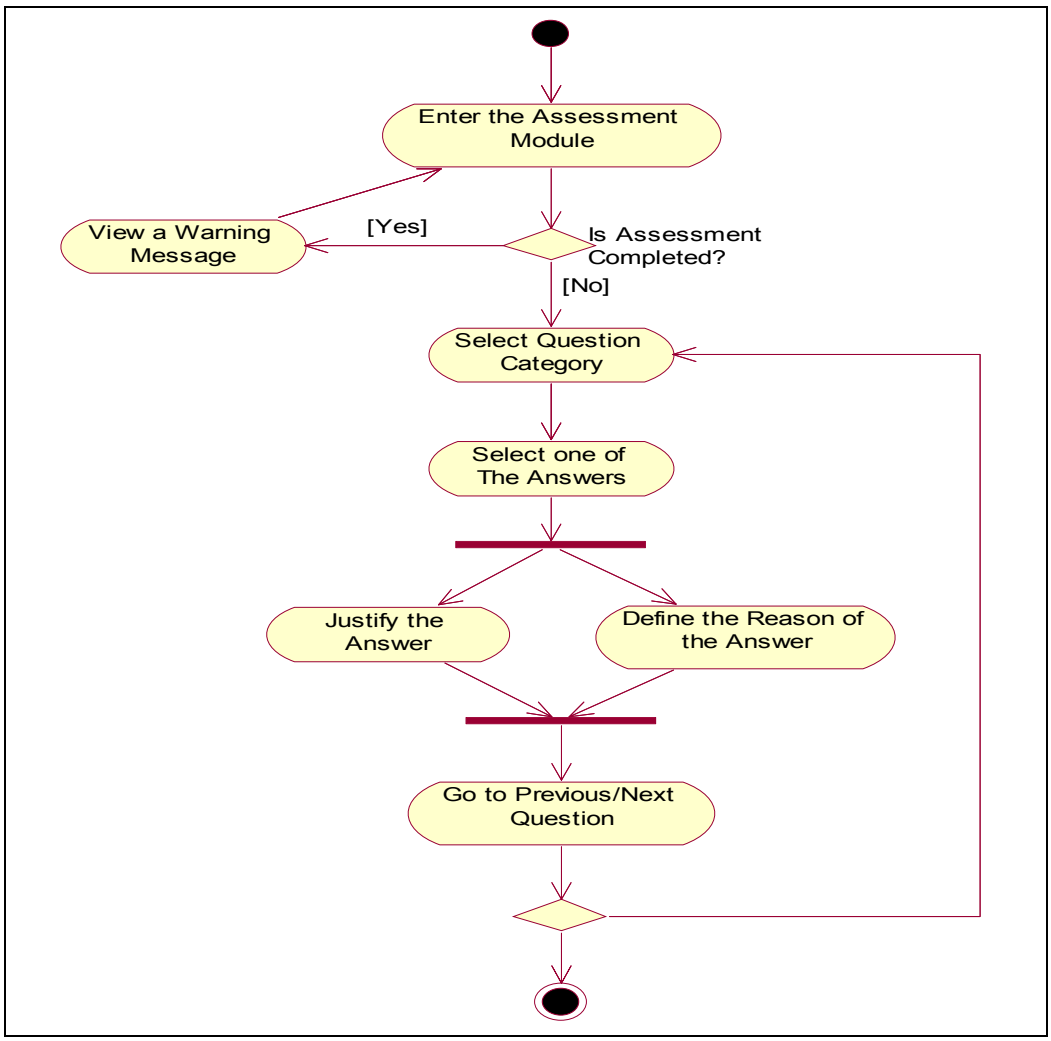


Figure 36 – Research Module Activity Diagram

CHAPTER 5

JUSTIFICATION

Although Infosec Toolkit is ready for use as a tool, it has not been commercialized yet. Also, it has not been evaluated in real life, or there is no help prepared for the tool and so on. On the other hand to establish an ISMS in an organization takes at least 3 months either with Infosec Toolkit or other toolset or without help of any software. Because of the reasons mentioned above Infosec Toolkit has not been justified as yet. But a case study is prepared for partial justification of the tool. This case study is given in the following section.

Since there should be some arrangements with DPT (Devlet Planlama Teşkiatı), research framework has not been justified yet either. These arrangements have not been made yet. But the application is setup on a server in Informatics Institute of METU and ready for use. The address of the web page is http://gapanalysis.ii.metu.edu.tr.

5.1 An imaginary case study for Infosec Toolkit

An imaginary organization is used for the case study. This organization is named as AE Turizm A.Ş. This company is a tourism agency. This company is based at an

office in Ankara, which customers can visit to make travel arrangements. The company has seven employees. All customer and travel related information and all information processing facilities used by the company are housed in this office. In addition to making travel arrangements in person at the office of AE Turizm A.Ş. customers can also make bookings on-line via the company's Web site.

AE Turizm A.Ş. offers the following services: arranging and booking of flights, hotels, car rental, and package holidays. AE Turizm A.Ş. also provides information to its customers about travel conditions, passport and visa requirements, health requirements about individual countries, weather and climate, airport details and foreign currencies.

Infosec Toolkit is used for the imaginary company described shortly above. Documents required for an ISMS are generated for AE Turizm A.Ş. Figures and descriptions of the processes used for the company is given in the following pages.

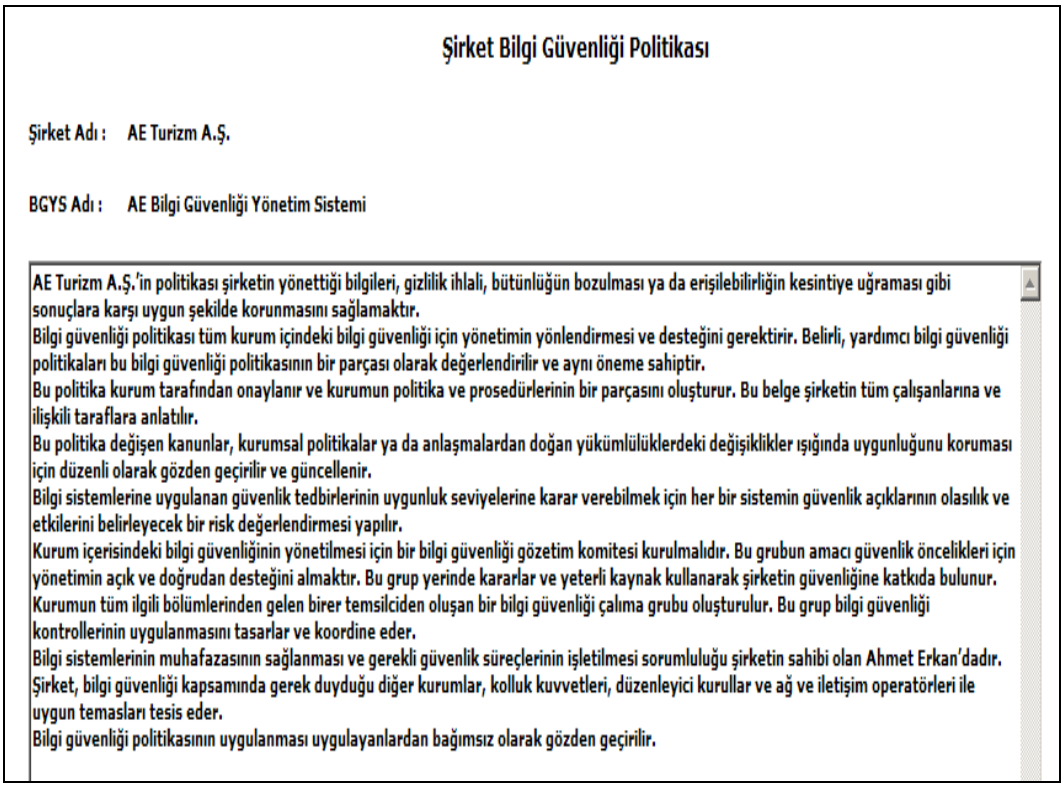
At first company defines its ISMS details. It is given in Figure 37.

Bilgi Güvenliği Yönetimi Sistemi Bilgileri

Şirket Adı :	AE Turizm A.Ş.
BGYS Adı :	AE Bilgi Güvenliği Yönetim Sistemi
BGYS'nin Açıklaması :	BGYS'nin kapsamı AE Turizm A.Ş. isimli şirketinden oluşmaktadır. Müşterilerinin seyahat düzenlemeleri ve rezervasyonlarını yapabildikleri Ankara'da konuşlu bir şirkettir. Bu şirketin sahibi bir kişidir ve çalışan sayısı 7'dir. Tüm müşteri ve seyahat bilgileri ve şirket tarafından kullanılan bilgi işleme araçları bu ofiste bulunmaktadır. Müşteriler doğrudan bu ofisten seyahat düzenlemeleri ve rezervasyonları yapabildikleri gibi şirketin web sayfasından da bu işlemleri yapabilmektedirler. AE Turizm A.Ş. tarafından uçuş, hotel, araba kiralama, paket tatiller vs. düzenleme ve rezervasyon hizmetleri sunmaktadır. Ayrıca şirket müşterilerini seyahat yapılacak ülkenin seyahat şartları, pasaport ve viza gereksinimleri, sağlık gereksinimleri, hava ve iklim durumu, hava alanı ayrıntıları ve döviz kurları hakkında da bilgilendirir. Ancak şirket döviz alım satımı ya da pasaport ve viza hizmetleri sunmamaktadır. Bu BGYS'de bulunan varlıkların ayrıntılı dökümü varlık envanterinde bulunabilir.
BGYS'nin Arayüzleri :	AE Turizm BGYS'nin arayüzleri şunlardır: - Şirketin ofisini ya da web sayfasını ziyaret eden müşteriler, - Havayolları, hoteller, araba kiralama şirketleri, ve diğer seyahat hizmetleri sunan şirketler, - Sigorta şirketleri, - Vergi makamları, - Müşterilerin ödemeleri ile ilişkili olan kredi kartı şirketeri ve bankalar, - Şirketin web sayfasını barındıran internet servis sağlayıcı, - Web sayfasının geliştirilmesini ve bakım hizmetlerini sunan şirket, - Ağ kurulumu, problem çıkması halinde Bilgi Teknolojileri ortamının bakımı gibi BT hizmetleri sunan şirket, - Ofis için elektrik, su vs. gibi ihtiyaçları sağlayan tesisatlar.
BGYS'nin Bağımlılıkları :	AE Turizm BGYS'nin bağımlı olduğu üçüncü taraf hizmet sağlayıcılar şunlardır: - Doğru rezervasyon işlemlerinin yapılmasını için havayolları, hoteller, araba kiralama şirketleri ve diğer seyahat şirketlerinden hizmetlerin ve kesin bilgilerin zamanında sağlanması, - Ödeme hizmetleri şirketlerinden zamanında provizon alınması, - İnternet servis sağlayıcısının web sayfasını müşterilere herzaman güvenli, doğru ve erişilebilir tutması, - Ofis için elektrik, su hizmetlerinin güvenli bir şekilde tedarik edilmesi.

Figure 37 – ISMS details of AE Turizm A.Ş.

Company's Information Security Policy is described by using Policy Module of Infosec Toolkit. This document is given Figure 38.


Şirket Bilgi Güvenliği Politikası

Şirket Adı : AE Turizm A.Ş.

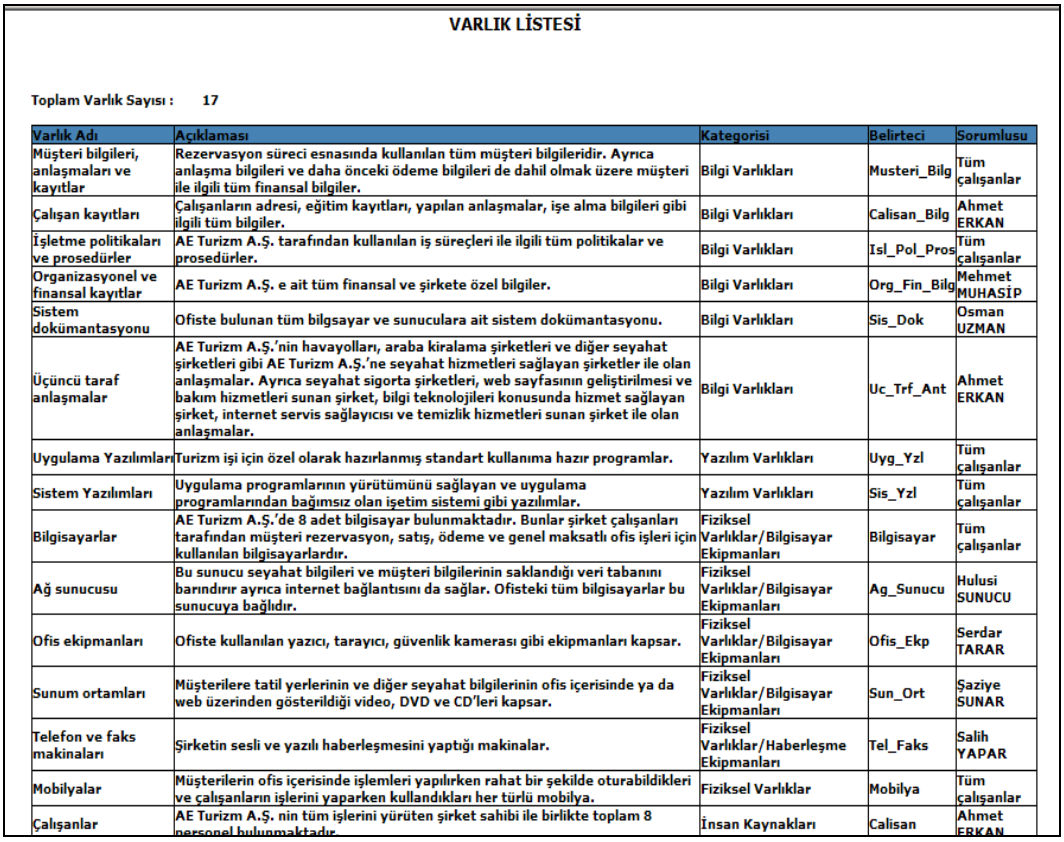
BGYS Adı : AE Bilgi Güvenliği Yönetim Sistemi

AE Turizm A.Ş.'in politikası şirketin yönettiği bilgileri, gizlilik ihlali, bütünlüğün bozulması ya da erişilebilirliğin kesintiye uğraması gibi sonuçlara karşı uygun şekilde korunmasını sağlamaktır.
Bilgi güvenliği politikası tüm kurum içindeki bilgi güvenliği için yönetimin yönlendirmesi ve desteğini gerektirir. Belirli, yardımcı bilgi güvenliği politikaları bu bilgi güvenliği politikasının bir parçası olarak değerlendirilir ve aynı öneme sahiptir.
Bu politika kurum tarafından onaylanır ve kurumun politika ve prosedürlerinin bir parçasını oluşturur. Bu belge şirketin tüm çalışanlarına ve ilişkili taraflara anlatılır.
Bu politika değişen kanunlar, kurumsal politikalar ya da anlaşmalardan doğan yükümlülüklerdeki değişiklikler ışığında uygunluğunu koruması için düzenli olarak gözden geçirilir ve güncellenir.
Bilgi sistemlerine uygulanan güvenlik tedbirlerinin uygunluk seviyelerine karar verebilmek için her bir sistemin güvenlik açıklarının olasılık ve etkilerini belirleyecek bir risk değerlendirmesi yapılır.
Kurum içerisindeki bilgi güvenliğinin yönetilmesi için bir bilgi güvenliği gözetim komitesi kurulmalıdır. Bu grubun amacı güvenlik öncelikleri için yönetimin açık ve doğrudan desteğini almaktır. Bu grup yerinde kararlar ve yeterli kaynak kullanarak şirketin güvenliğine katkıda bulunur.
Kurumun tüm ilgili bölümlerinden gelen birer temsilciden oluşan bir bilgi güvenliği çalıma grubu oluşturulur. Bu grup bilgi güvenliği kontrollerinin uygulanmasını tasarlar ve koordine eder.
Bilgi sistemlerinin muhafazasının sağlanması ve gerekli güvenlik süreçlerinin işletilmesi sorumluluğu şirketin sahibi olan Ahmet Erkan'dadır.
Şirket, bilgi güvenliği kapsamında gerek duyduğu diğer kurumlar, kolluk kuvvetleri, düzenleyici kurullar ve ağ ve iletişim operatörleri ile uygun temasları tesis eder.
Bilgi güvenliği politikasının uygulanması uygulayanlardan bağımsız olarak gözden geçirilir.

Figure 38 – Information Security Policy of the Company

After defining the perimeter of ISMS and organization's Information Security Policy, company identifies its assets. Asset inventory of AE Turizm A.Ş. composed by the tool is given in Figure 39.

In the next step company defines its security requirements, threats, vulnerabilities, risks, selected controls and controls which are not selected and the rationale for them are defined successively. Some portions of risk list, selected controls list and non selected controls list are given as exemplary.

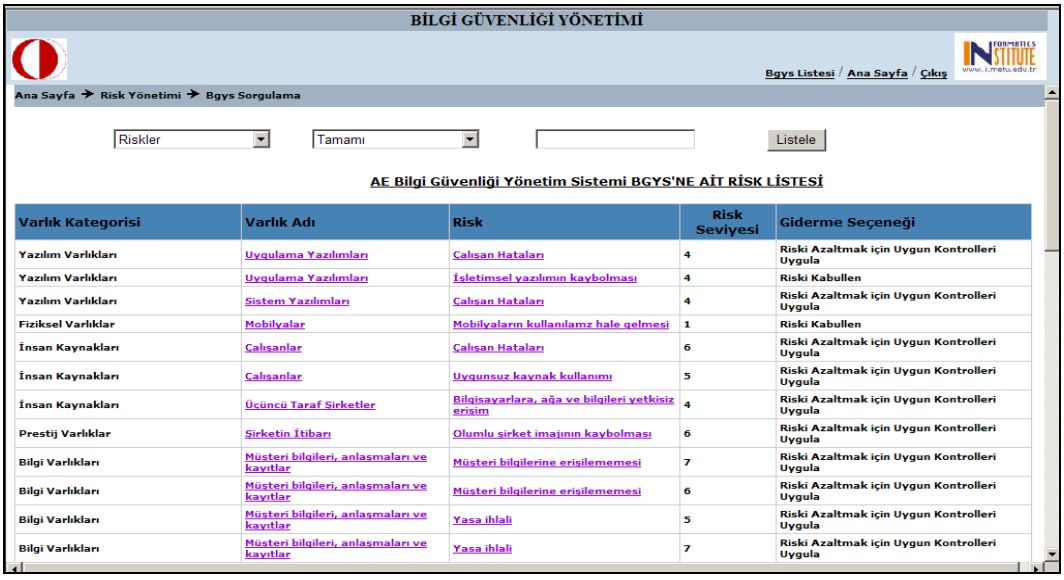


VARLIK LİSTESİ

Toplam Varlık Sayısı : 17

Varlık Adı	Açıklaması	Kategorisi	Belirteci	Sorumlusu
Müşteri bilgileri, anlaşmaları ve kayıtlar	Rezervasyon süreci esnasında kullanılan tüm müşteri bilgileridir. Ayrıca anlaşma bilgileri ve daha önceki ödeme bilgileri de dahil olmak üzere müşteri ile ilgili tüm finansal bilgiler.	Bilgi Varlıkları	Musteri_Bilg	Tüm çalışanlar
Çalışan kayıtları	Çalışanların adresi, eğitim kayıtları, yapılan anlaşmalar, işe alma bilgileri gibi ilgili tüm bilgiler.	Bilgi Varlıkları	Calisan_Bilg	Ahmet ERKAN
İşletme politikaları ve prosedürler	AE Turizm A.Ş. tarafından kullanılan iş süreçleri ile ilgili tüm politikalar ve prosedürler.	Bilgi Varlıkları	Isl_Pol_Pros	Tüm çalışanlar
Organizasyonel ve finansal kayıtlar	AE Turizm A.Ş. e ait tüm finansal ve şirkete özel bilgiler.	Bilgi Varlıkları	Org_Fin_Bilg	Mehmet MUHASİP
Sistem dokümantasyonu	Ofiste bulunan tüm bilgsayar ve sunuculara ait sistem dokümantasyonu.	Bilgi Varlıkları	Sis_Dok	Osman UZMAN
Üçüncü taraf anlaşmalar	AE Turizm A.Ş.'nin havayolları, araba kiralama şirketleri ve diğer seyahat şirketleri gibi AE Turizm A.Ş.'ne seyahat hizmetleri sağlayan şirketler ile olan anlaşmalar. Ayrıca seyahat sigorta şirketleri, web sayfasının geliştirilmesi ve bakım hizmetleri sunan şirket, bilgi teknolojileri konusunda hizmet sağlayan şirket, internet servis sağlayıcısı ve temizlik hizmetleri sunan şirket ile olan anlaşmalar.	Bilgi Varlıkları	Uc_Trf_Ant	Ahmet ERKAN
Uygulama Yazılımları	Turizm işi için özel olarak hazırlanmış standart kullanıma hazır programlar.	Yazılım Varlıkları	Uyg_Yzl	Tüm çalışanlar
Sistem Yazılımları	Uygulama programlarının yürütümünü sağlayan ve uygulama programlarından bağımsız olan işetim sistemi gibi yazılımlar.	Yazılım Varlıkları	Sis_Yzl	Tüm çalışanlar
Bilgisayarlar	AE Turizm A.Ş.'de 8 adet bilgisayar bulunmaktadır. Bunlar şirket çalışanları tarafından müşteri rezervasyon, satış, ödeme ve genel maksatlı ofis işleri için kullanılan bilgisayarlardır.	Fiziksel Varlıklar/Bilgisayar Ekipmanları	Bilgisayar	Tüm çalışanlar
Ağ sunucusu	Bu sunucu seyahat bilgileri ve müşteri bilgilerinin saklandığı veri tabanını barındırır ayrıca internet bağlantısını da sağlar. Ofisteki tüm bilgisayarlar bu sunucuya bağlıdır.	Fiziksel Varlıklar/Bilgisayar Ekipmanları	Ag_Sunucu	Hulusi SUNUCU
Ofis ekipmanları	Ofiste kullanılan yazıcı, tarayıcı, güvenlik kamerası gibi ekipmanları kapsar.	Fiziksel Varlıklar/Bilgisayar Ekipmanları	Ofis_Ekp	Serdar TARAR
Sunum ortamları	Müşterilere tatil yerlerinin ve diğer seyahat bilgilerinin ofis içerisinde ya da web üzerinden gösterildiği video, DVD ve CD'leri kapsar.	Fiziksel Varlıklar/Bilgisayar Ekipmanları	Sun_Ort	Şaziye SUNAR
Telefon ve faks makinaları	Şirketin sesli ve yazılı haberleşmesini yaptığı makinalar.	Fiziksel Varlıklar/Haberleşme Ekipmanları	Tel_Faks	Salih YAPAR
Mobilyalar	Müşterilerin ofis içerisinde işlemleri yapılırken rahat bir şekilde oturabildikleri ve çalışanların işlerini yaparken kullandıkları her türlü mobilya.	Fiziksel Varlıklar	Mobilya	Tüm çalışanlar
Çalışanlar	AE Turizm A.Ş. nin tüm işlerini yürüten şirket sahibi ile birlikte toplam 8 personel bulunmaktadır.	İnsan Kaynakları	Calisan	Ahmet ERKAN

Figure 39 – Asset Inventory



BİLGİ GÜVENLİĞİ YÖNETİMİ

Bgys Listesi / Ana Sayfa / Çıkış

Ana Sayfa → Risk Yönetimi → Bgys Sorgulama

Riskler | Tamamı | Listele

AE Bilgi Güvenliği Yönetim Sistemi BGYS'NE AİT RİSK LİSTESİ

Varlık Kategorisi	Varlık Adı	Risk	Risk Seviyesi	Giderme Seçeneği
Yazılım Varlıkları	Uygulama Yazılımları	Çalışan Hataları	4	Riski Azaltmak için Uygun Kontrolleri Uygula
Yazılım Varlıkları	Uygulama Yazılımları	İşletimsel yazılımın kaybolması	4	Riski Kabullen
Yazılım Varlıkları	Sistem Yazılımları	Çalışan Hataları	4	Riski Azaltmak için Uygun Kontrolleri Uygula
Fiziksel Varlıklar	Mobilyalar	Mobilyaların kullanılamz hale gelmesi	1	Riski Kabullen
İnsan Kaynakları	Çalışanlar	Çalışan Hataları	6	Riski Azaltmak için Uygun Kontrolleri Uygula
İnsan Kaynakları	Çalışanlar	Uygunsuz kaynak kullanımı	5	Riski Azaltmak için Uygun Kontrolleri Uygula
İnsan Kaynakları	Üçüncü Taraf Şirketler	Bilgisayarlara, ağa ve bilgileri yetkisiz erişim	4	Riski Azaltmak için Uygun Kontrolleri Uygula
Prestij Varlıklar	Şirketin İtibarı	Olumlu şirket imajının kaybolması	6	Riski Azaltmak için Uygun Kontrolleri Uygula
Bilgi Varlıkları	Müşteri bilgileri, anlaşmaları ve kayıtlar	Müşteri bilgilerine erişilememesi	7	Riski Azaltmak için Uygun Kontrolleri Uygula
Bilgi Varlıkları	Müşteri bilgileri, anlaşmaları ve kayıtlar	Müşteri bilgilerine erişilememesi	6	Riski Azaltmak için Uygun Kontrolleri Uygula
Bilgi Varlıkları	Müşteri bilgileri, anlaşmaları ve kayıtlar	Yasa ihlali	5	Riski Azaltmak için Uygun Kontrolleri Uygula
Bilgi Varlıkları	Müşteri bilgileri, anlaşmaları ve kayıtlar	Yasa ihlali	7	Riski Azaltmak için Uygun Kontrolleri Uygula

Figure 40 – Risk List

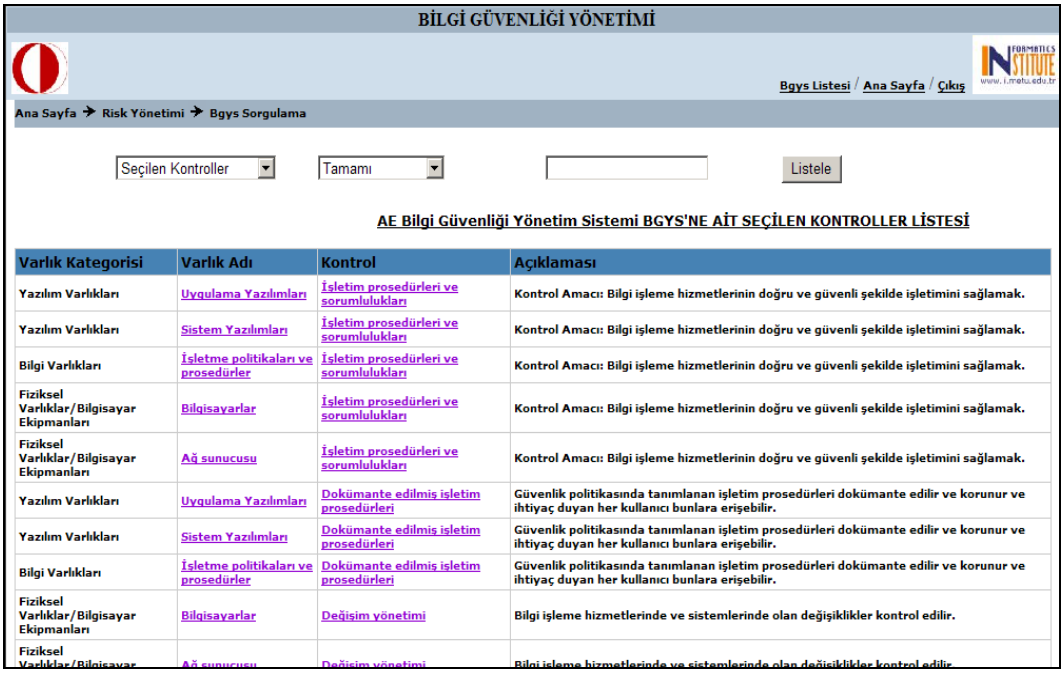


Figure 41 – Selected Controls List

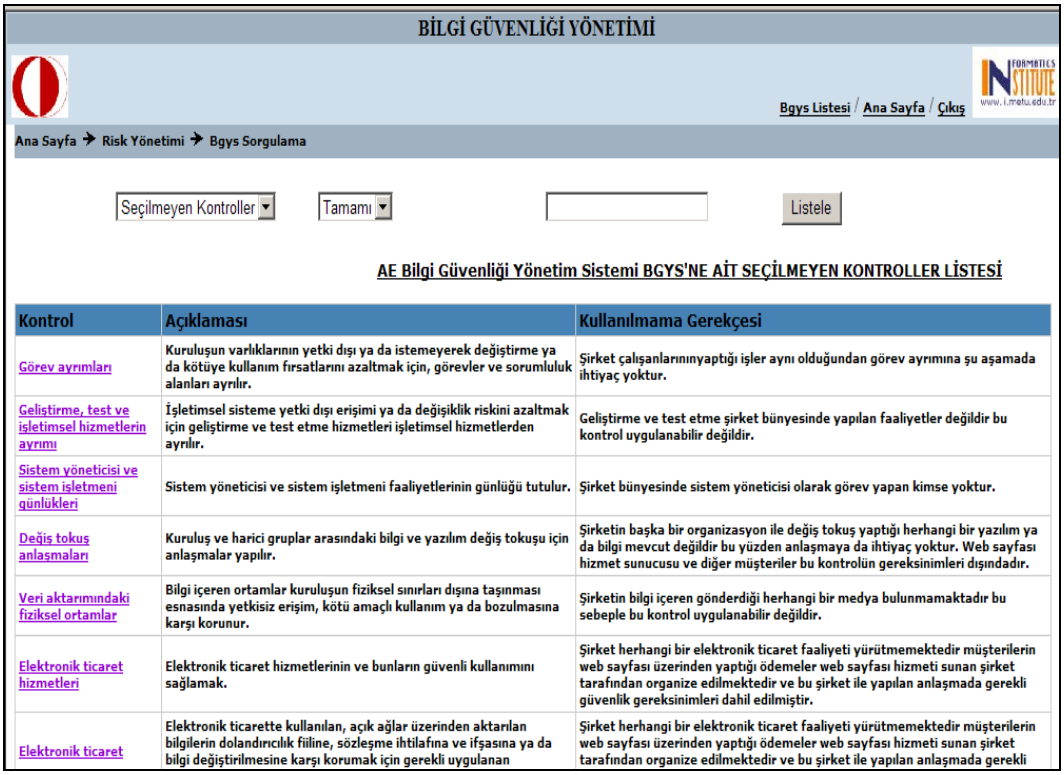


Figure 42 – List of Non Selected Controls

All of this information is generated by using Risk Management Module. After the generation this information, it can be view by using Query and Reporting Module.

Other documents generated for AE Turizm A.Ş such as Statement of Applicability, Risk Assessment Report, Risk Treatment Plan, and Review of Controls Implementation Levels, are given in the following figures.

UYGULANABİLİRLİK BEYANNAMESİ

5. GÜVENLİK POLİTİKASI

5.1. Bilgi Güvenliği Politikası

5.1.1.Yönetim tarafından onaylanmış hazırlanan bilgi güvenliği dokümanı tüm çalışanlara ve ilgili harici gruplara yayınlanIR ve iletilir.

Uygulanıyor

Azalttığı Risk Listesi

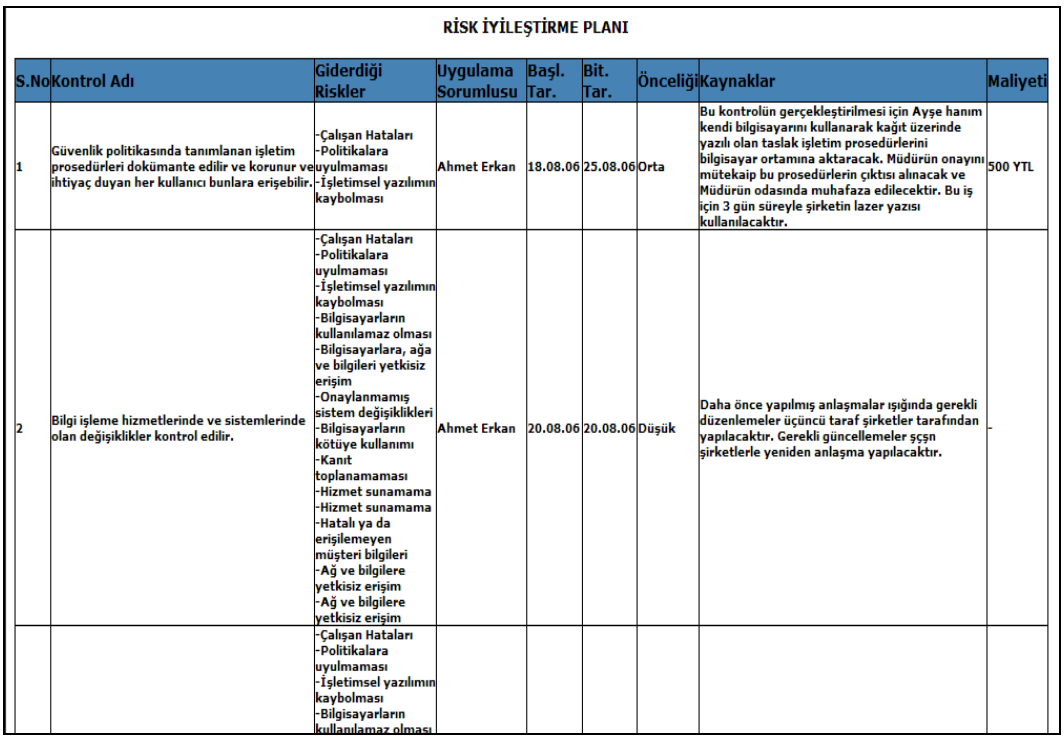
S.No	Azalttığı Risk	İlişkili Olduğu Tehdit/Hassasiyetler	Kategorisi	Önceki Risk Seviyesi	İndirgediği Risk Seviyesi	Açıklama
1	Çalışan Hataları	Çalışan hataları ya da yanlış hareketleri/Zamana uygun eğitimin eksikliği	İnsan	6	3	Yerinde eğitimlerin verilmesi ve şirket içerisinde güvenlik kültürünün oluşturulması ile çalışan hataları azaltılır ve ayrıca oluşacak problemler ve etkileri de sınırlandırılır.
2	Uygunsuz kaynak kullanımı	Yetersiz personel/Uygun çalışan ayarlamalarının yapılmaması	İnsan	5	4	Görev başında olacak personel için uygun düzenlemelerin yapılması ile yetersiz personel ile işi sürdürme gibi bir durum ortadan kalkacaktır.
3	Politikalara uyulmaması	Şirket içi politika ve prosedürlerin önemsenmemesi/Bu dokümanların eksik ya da güncel olmaması	İnsan	6	3	Politikaların gözden geçirilmesi ve güncellenmesi eksiksiz ve güncel olmalarını sağlayacaktır. Politikalara uygunluğun kontrol edilmesi çalışanlara bu politikaların önemli olduğunu ve uyulması gerektiğini gösterecektir. Ayrıca politika ve prosedürlerin değiştirilmesi sorunun etkisini de azaltacaktır.
4	Politikalara uyulmaması	Şirket içi politika ve prosedürlerin önemsenmemesi/Eğitim eksikliği	İnsan	6	4	Bu kontrollerin uygulanması politika ve prosedürlerin göz ardı edilmesini oldukça azaltacaktır. Eğitim ile bu durum daha da iyileştirilecektir.
5	Bilgisayarların kullanılamaz olması	Yangın/Yangın karşı önlemlerin eksikliği	Fiziksel ve Çevresel	4	2	Bu kontroller yangına karşı korumayı artıracaktır ve yangın çıkması durumunda etki iş sürekliliği kontrolleri etkiyi azaltacaktır.
6	Bilgisayarların kullanılamaz olması	Güç kaynağının arızalanması/Güç kaynağının düzgün şekilde çalışmaması	Fiziksel ve Çevresel	5	4	Bu kontrollerin uygulanması bu tür arızaları azaltacaktır.
7	Bilgisayarlara, ağa ve bilgileri yetkisiz erişim	Bilgisayarlara yetkisiz kişilerce erişilmesi/Boş bilgisayarlar için yetersiz koruma önlemleri	Erişim Kontrolü	7	5	Bu problemin giderilmesi için gerekli her şey belirtilmiştir. Tüm kontroller bir kere uygulandıktan sonra problemin ortaya çıkma olasılığını azaltacaktır. Fakat yine de böyle bir problemle karşılaşılabilir ancak bu risk daha fazla azaltılamamaktadır.
8	Onaylanmamış sistem değişiklikleri	Yetkisiz yazılım kurulması ya da yazılımlarda değişiklik yapılması/Kurulumların	Sistem Geliştirme ve Bakımı	7	3	Bu kontrollerin uygulanması yetkisiz yazılım kurulumları olasılığını azaltacaktır ve önceki durumun kopyasının alınması ile böyle bir yükleme olsa bile oluşacak hasarı önleyecektir.

Figure 43 – Statement of Applicability

RİSK DEĞERLENDİRME RAPORU

S. No	Risk Adı	İlişkili Olduğu Tehdit/Hassasiyetler	Risk Seviyesi	İyileştirme Seçeneği
1	Müşteri bilgilerine erişilememesi	Müşteri bilgilerinin silinmesi/Çalışan hataları	7	Riski Azaltmak için Uygun Kontrolleri Uygula
2	Yasa ihlali	Müşteri bilgileri ile ilgili yasalara uymamak/Çalışanların bu konuda yeterli bilgiye sahip olmaması	7	Riski Azaltmak için Uygun Kontrolleri Uygula
3	Yasa ihlali	Müşteri bilgileri ile ilgili yasalara uymamak/Ağ güvenliğinin yetersizliği	7	Riski Azaltmak için Uygun Kontrolleri Uygula
4	Yasa ihlali	Çalışan bilgileri ile ilgili yasalara uymamak/Ağ güvenliğinin yetersizliği	7	Riski Azaltmak için Uygun Kontrolleri Uygula
5	Yasa ihlali	Kurumsal kayıtların imha edilmesi/Yedeklemelerin yetersizliği	7	Riski Azaltmak için Uygun Kontrolleri Uygula
6	Bilgisayarlara, ağa ve bilgileri yetkisiz erişim	Bilgisayarlara yetkisiz kişilerce erişilmesi/Boş bilgisayarlar için yetersiz koruma önlemleri	7	Riski Azaltmak için Uygun Kontrolleri Uygula
7	Onaylanmamış sistem değişiklikleri	Yetkisiz yazılım kurulması ya da yazılımlarda değişiklik yapılması/Kurulumların denetlenmemesi	7	Riski Azaltmak için Uygun Kontrolleri Uygula
8	Bilgisayarların kötüye kullanımı	Bilgisayarlara yetkisiz kullanılması/Politika eksikliği	7	Riski Azaltmak için Uygun Kontrolleri Uygula
9	Hizmet sunamama	Hizmetin engellenmesi/Gerçek istekleri sahte olanlardan ayırt edememe	7	Riski ya da Doğabilecek Maddi Sonuçları Transfer Et
10	Ağ ve bilgilere yetkisiz erişim	Ağ üzerinden yetkisiz erişim/Tarihi geçmiş firewall konfigürasyonu	7	Riski Azaltmak için Uygun Kontrolleri Uygula
11	Hatalı ya da erişilemeyen müşteri bilgileri	Sunucu hatası/Yedeklemelerin yetersizliği	6	Riski Azaltmak için Uygun Kontrolleri Uygula
12	Ağ ve bilgilere yetkisiz erişim	Ağ üzerinden yetkisiz erişim/Bilinmeyen kötü amaçlı yazılımlar	6	Riski Azaltmak için Uygun Kontrolleri Uygula
13	Anlaşmalara erişilememesi	Üçüncü taraf anlaşmaların imha edilmesi/Korumasız depolama	6	Riski Azaltmak için Uygun Kontrolleri Uygula
14	Yasa ihlali	Kurumsal kayıtların imha edilmesi/Eski kayıtların yetersiz bir şekilde kontrol edilmesi	6	Riski Azaltmak için Uygun Kontrolleri Uygula
15	Yasa ihlali	Çalışan bilgileri ile ilgili yasalara uymamak/Korunmayan kayıtlar	6	Riski Azaltmak için Uygun Kontrolleri Uygula

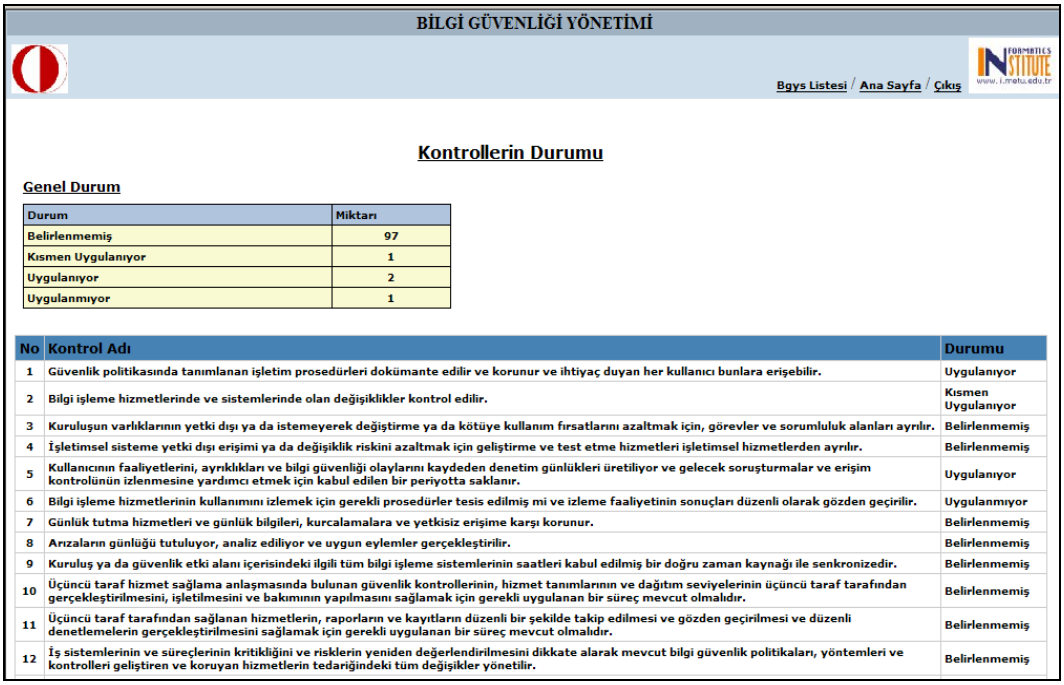
Figure 44 – Risk Assessment Report



RİSK İYİLEŞTİRME PLANI

S.No	Kontrol Adı	Giderdiği Riskler	Uygulama Sorumlusu	Başl. Tar.	Bit. Tar.	Önceliği	Kaynaklar	Maliyeti
1	Güvenlik politikasında tanımlanan işletim prosedürleri dokümante edilir ve korunur ve ihtiyaç duyan her kullanıcı bunlara erişebilir.	-Çalışan Hataları -Politikalara uyulmaması -İşletimsel yazılımın kaybolması	Ahmet Erkan	18.08.06	25.08.06	Orta	Bu kontrolün gerçekleştirilmesi için Ayşe hanım kendi bilgisayarını kullanarak kağıt üzerinde yazılı olan taslak işletim prosedürlerini bilgisayar ortamına aktaracak. Müdürün onayını mütekaip bu prosedürlerin çıktısı alınacak ve Müdürün odasında muhafaza edilecektir. Bu iş için 3 gün süreyle şirketin lazer yazısı kullanılacaktır.	500 YTL
2	Bilgi işleme hizmetlerinde ve sistemlerinde olan değişiklikler kontrol edilir.	-Çalışan Hataları -Politikalara uyulmaması -İşletimsel yazılımın kaybolması -Bilgisayarların kullanılamaz olması -Bilgisayarlara, ağa ve bilgileri yetkisiz erişim -Onaylanmamış sistem değişiklikleri -Bilgisayarların kötüye kullanımı -Kanıt toplanamaması -Hizmet sunamama -Hizmet sunamama -Hatalı ya da erişilemeyen müşteri bilgileri -Ağ ve bilgilere yetkisiz erişim -Ağ ve bilgilere yetkisiz erişim	Ahmet Erkan	20.08.06	20.08.06	Düşük	Daha önce yapılmış anlaşmalar ışığında gerekli düzenlemeler üçüncü taraf şirketler tarafından yapılacaktır. Gerekli güncellemeler şçşn şirketlerle yeniden anlaşma yapılacaktır.	-
		-Çalışan Hataları -Politikalara uyulmaması -İşletimsel yazılımın kaybolması -Bilgisayarların kullanılamaz olması						

Figure 45 – Risk Treatment Plan



BİLGİ GÜVENLİĞİ YÖNETİMİ

Bgys Listesi / Ana Sayfa / Çıkış

Kontrollerin Durumu

Genel Durum

Durum	Miktarı
Belirlenmemiş	97
Kısmen Uygulanıyor	1
Uygulanıyor	2
Uygulanmıyor	1

No	Kontrol Adı	Durumu
1	Güvenlik politikasında tanımlanan işletim prosedürleri dokümante edilir ve korunur ve ihtiyaç duyan her kullanıcı bunlara erişebilir.	Uygulanıyor
2	Bilgi işleme hizmetlerinde ve sistemlerinde olan değişiklikler kontrol edilir.	Kısmen Uygulanıyor
3	Kuruluşun varlıklarının yetki dışı ya da istemeyerek değiştirme ya da kötüye kullanım fırsatlarını azaltmak için, görevler ve sorumluluk alanları ayrılır.	Belirlenmemiş
4	İşletimsel sisteme yetki dışı erişimi ya da değişiklik riskini azaltmak için geliştirme ve test etme hizmetleri işletimsel hizmetlerden ayrılır.	Belirlenmemiş
5	Kullanıcının faaliyetlerini, ayrıklıkları ve bilgi güvenliği olaylarını kaydeden denetim günlükleri üretiliyor ve gelecek soruşturmalar ve erişim kontrolünün izlenmesine yardımcı etmek için kabul edilen bir periyotta saklanır.	Uygulanıyor
6	Bilgi işleme hizmetlerinin kullanımını izlemek için gerekli prosedürler tesis edilmiş mi ve izleme faaliyetinin sonuçları düzenli olarak gözden geçirilir.	Uygulanmıyor
7	Günlük tutma hizmetleri ve günlük bilgileri, kurcalamalara ve yetkisiz erişime karşı korunur.	Belirlenmemiş
8	Arızaların günlüğü tutuluyor, analiz ediliyor ve uygun eylemler gerçekleştirilir.	Belirlenmemiş
9	Kuruluş ya da güvenlik etki alanı içerisindeki ilgili tüm bilgi işleme sistemlerinin saatleri kabul edilmiş bir doğru zaman kaynağı ile senkronizedir.	Belirlenmemiş
10	Üçüncü taraf hizmet sağlama anlaşmasında bulunan güvenlik kontrollerinin, hizmet tanımlarının ve dağıtım seviyelerinin üçüncü taraf tarafından gerçekleştirilmesini, işletilmesini ve bakımının yapılmasını sağlamak için gerekli uygulanan bir süreç mevcut olmalıdır.	Belirlenmemiş
11	Üçüncü taraf tarafından sağlanan hizmetlerin, raporların ve kayıtların düzenli bir şekilde takip edilmesi ve gözden geçirilmesi ve düzenli denetlemelerin gerçekleştirilmesini sağlamak için gerekli uygulanan bir süreç mevcut olmalıdır.	Belirlenmemiş
12	İş sistemlerinin ve süreçlerinin kritikliğini ve risklerin yeniden değerlendirilmesini dikkate alarak mevcut bilgi güvenlik politikaları, yöntemleri ve kontrolleri geliştiren ve koruyan hizmetlerin tedariğindeki tüm değişikler yönetilir.	Belirlenmemiş

Figure 46 – Status of Controls

CHAPTER 6

CONCLUSIONS

Information security's management aspect is gaining more and more interest in the world as mentioned in section 2.8. Although current situation in Turkey is not so much different, comparing with Japan, UK or India, Turkey has a lot to do in this field.

In the scope of this thesis, two tools are created to fulfill two different missions with the aim of helping Turkish organizations. These are Infosec Toolkit and Research Framework.

If organizations want to do business internationally, it is more important to emphasize information security management in the management process. In order to prove that the organization has sufficient information security safeguards against threats, having certification of ISO/IEC 27001:2005 is one of the best ways. Thus, to have certification of ISO/IEC 27001:2005 makes it easy to do business internationally. One of the aims of this study has been to offer a toolkit to organizations for their information security management process to automate activities required for a documented ISMS as much as possible.

There are various tools developed in order to help organizations during the ISMS process or in a general manner for information security issues. There are not so many tools helping organizations to construct the information security or to establish an ISMS as a complete manner. As mentioned in section 2.8, most of the tools concentrate on one or a couple of specific areas. Most of them are concentrated on a specific scope of information security. Although using a tool which concentrates on a specific area can be useful, using a more comprehensive tool which helps in all aspects of information security and ISMS process can be more advantageous. But Infoce Toolkit is a comprehensive tool. Organizations can use this tool for risk management, policy management, initial gap analysis, monitoring and query and reporting as a complete manner.

Since new versions of ISO/IEC 27001:2005 and ISO/IEC 17799:2005 was published in 2005, most of the tools developed in this scope have become out of date. Infosec Toolkit is contemporary.

To adopt ISO/IEC 27001:2005 is a complicated process and needs so much time and money. Using Infosec Toolkit, organizations can fulfill the requirements of ISO/IEC 27001:2005 easily. In addition, to use Infosec Toolkit reduces adoption time and the expenses in a reasonable degree.

In addition there is no tool developed in Turkish except BizNet's ISMart. Since the aim this study has been to contribute Turkish organizations in the information security field, usability of the tools used by Turkish organizations is important. And considering the growth rate of interest in information security's management aspect, it can be said that the number of tools especially developed in Turkish thus used by Turkish organizations easily is limited. So it is important for Turkish organizations especially for public organizations to have a tool having Turkish interfaces. That is why Infosec Toolkit is prepared in Turkish.

The other aim of the thesis has been to introduce a framework to take the picture of current situations of public and private organizations about Information Security in Turkey. That is why this tool has been developed in Turkish, too.

6.1 Future Work

Infosec Toolkit may be commercialized by adding help for the tool. After commercialized, this tool will close a gap in this area in Turkey. As this tool is used by organizations, some information security data which is not so critical for organizations can be retrieved from the organizations in order to be used to generate general report on information security issues like CSI/FBI Surveys periodically.

As mentioned above only Qualitative Risk Assessment Methodology is used in the scope of this tool, it can be added Quantitative Methodology. And a capability that organization can choose from methodologies of which fits its needs can be added.

In this toolkit there are no capabilities used for increasing the awareness and education level of employees. In order to do so there can be added a module that helps educating the employees in information security on the exact level relevant for every group of employees. It can be e-learning based information security education. Users can have exams, read some papers, and watch videos about information security etc.

There is only one user role for the system. There can be defined some roles such as upper management, information security officer, and end user etc. managers can generate reports on information security of the organization. Information security officer can manage the system by managing incident, evaluating the risks according to the threats and vulnerabilities, create risk assessment report, etc. and end user can report incidents by filling incident report form, in addition end user

can perform some task such as defining assets, requirements, threats, vulnerabilities etc.

In the Initial Gap Analysis and Monitoring Module, there exists only two assessment booklet. A module, that a user can create new assessment booklets according to the organization's needs, can be added.

As for Research Module, there are also some improvements for this module. Although this module is setup on a server in Informatics Institute of METU and ready for use, it is not being used officially. It will be used after the required arrangements are made. The information gathered using this application, can be used to generate annual or semiannual reports like CSI/FBI Surveys.
This application uses only ISO/IEC 27001:2005 Information Security Initial Gap Analysis. It would be useful to extend the application to contain other assessment booklet presented in this thesis, Assessment of ISMS Process Requirements. In addition some other test booklets can be added.

And lastly, since the aim of this thesis is to help Turkish organization in information security, both Infosec Toolkit and Research Module are prepared in Turkish. These tools can be prepared in some other languages like English in order to fulfill the requirements of globalization in the future.

REFERENCES

[1] ISO/IEC 17799:2005(E), Information technology — Security techniques — Code of practice for information security management

[2] ISO/IEC 27001:2005(E), Information technology — Security techniques — Information security management systems — Requirements

[3] Mjølsnes, S.F, Skramstad, T., Stålhane, T., Houmb, S.H. & Bratthall, L. (2004, April). System dependability and the future - INFOSAM2020, Norwegian University of Science and Technology. Retrieved August 02, 2006, from http://www.ime.ntnu.no/infosam2020/oldpage/work_groups/wg_information_security.html

[4] Gordon, L.A., Loeb, M.P, Lucyshyn, W. and Richardson, R. (2005). CSI/FBI Computer Crime and Security Survey, 2005, pp. 22.

[5] Guide to BS 7799 Risk Assessment (PD 3002) – Guidance aimed to those responsible for carrying out risk management. Edited by Humphreys, T. & Plate, A. Published by Delivering Information Solutions to Customers (Part of British Standards Institution responsible for standardization in Information and Communications Technologies). pp. 16-17.

[6] Kevin, H. (2003). Risk Management and Analysis. In Tipton, H. F. (Eds), Information Security Management Handbook (pp.751). Boca Raton, FL, USA: Auerbach Publishers, Incorporated.

[7] Peltier, T. R. (2001). Information Security Risk Analysis. Boca Raton, FL, USA: Auerbach Publishers, Incorporated.

[8] OECD. (2002), Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD.

[9] Gordon, L.A., Loeb, M.P, Lucyshyn, W. and Richardson, R. (2006). CSI/FBI Computer Crime and Security Survey, 2006. pp.18.

[10] PricewaterhouseCoopers on behalf of the UK Department of Trade and Industry. (2006). Information security breaches survey 2006 - technical report. Retrieved August 22, 2006, from http://www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16, pp. 9.

[11] Andersson, F.M. (2004). ISO/IEC 17799 Compliant? Master Thesis, Department of Computer and Systems Sciences Stockholm's University / Royal Institute of technology. pp. 13-14.

[12] ISO/IEC TR 13335-3:1998(E), Information technology — Guidelines for the management of IT Security — Techniques for the management of IT Security, pp. 8–9.

[13] ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management, pp.6-8.

[14] "Are you ready for a BS 7799 Audit? (DISC PD 3003) – A compliance assessment workbook". Edited by Humphreys, T. & Plate, A. Published by Delivering Information Solutions to Customers (Part of British Standards Institution responsible for standardization in Information and Communications Technologies).

[15] Kwok, L. & Dennis Longley, D. (1999). "Information security management and modeling". Journal: Information Management & Computer Security Volume: 7, pp. 30 – 40.

[16] NIST SP 800-53. (2006). “Information Security Handbook: A Guide for Managers”.

[17] Codd, E.F. (1970). "A Relational Model of Data for Large Shared Data Banks". Communications of the ACM 13 (6): pp. 377–387.

[18] Bayis, O.A. (2000). “Total Security Management – A Paradigm for Developing Secure Information Systems”, METU, Ankara, Turkey.

[19] Yücel, O (2001). “Information System Security”, METU, Ankara, Turkey.