



**YILDIRIM BEYAZIT UNIVERSITY  
GRADUATE SCHOOL OF NATURAL AND APPLIED  
SCIENCES**

**DEVELOPING A SEARCH TOOL FOR INFORMATION  
SECURITY MANAGEMENT SYSTEMS STANDARDS**

**M.Sc. Thesis by  
YASİN KARAPINAR**

**Department of Computer Engineering**

**June, 2016**

**ANKARA**



**Yasin KARAPINAR**

**Department of Computer Engineering**

**2016 ANKARA**

# **DEVELOPING A SEARCH TOOL FOR INFORMATION SECURITY MANAGEMENT SYSTEMS STANDARDS**

**A Thesis Submitted to  
the Graduate School of Natural and Applied Sciences of Yıldırım Beyazıt  
University**

**In Partial Fulfillment of the Requirements for the Degree of Master of Science  
in Computer Engineering, Department of Computer Engineering**

**by**

**Yasin KARAPINAR**

**June, 2016  
ANKARA**

## M.Sc. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled “DEVELOPING A SEARCH TOOL FOR INFORMATION SECURITY MANAGEMENT SYSTEMS STANDARDS” completed by Yasin KARAPINAR under supervision of Asst. Prof. Dr. Lami KAYA and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

.....  
\_\_\_\_\_  
**(Supervisor)**

.....  
\_\_\_\_\_  
**(Jury Member)**

.....  
\_\_\_\_\_  
**(Jury Member)**

.....  
\_\_\_\_\_  
**(Director)**

Graduate School of Natural and Applied Sciences

## ETİK BEYAN

Yıldırım Beyazıt Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

## **ACKNOWLEDGEMENTS**

First and above all, I praise my Lord that provides me countless opportunities.

I am deeply grateful for my supervisor Asst. Prof. Lami KAYA's significant contributions, crucial support, beneficial suggestions and sincere comments in the preparation of this overall study. He was always very understanding and positive in every stage of my graduate study.

I greatly thank my dear brother Nurettin SEZER from the bottom of my heart. He gave me valuable advice for this thesis and he allocated his valuable time to review and revise this thesis. I also thank warmly my friends Tugay ÖZSOY and Mustafa TEMEL who helped me by reviewing and proof reading this thesis.

I would like to send a huge thank you to my parents, Rahime and Satılmış for their endless support, encouragement and love. I am also grateful to my little darlings, Muhammed Emir and Nil Hüma, for the patience they have shown with their little loving hearts for every minute I have spent without them to prepare this thesis. Lastly, my greatest gratitude goes to my dear wife Fatma for her unbelievable patience, support, and love throughout the time I was writing this thesis.

2016, 7 June

Yasin KARAPINAR

# DEVELOPING A SEARCH TOOL FOR INFORMATION SECURITY MANAGEMENT SYSTEMS STANDARDS

## ABSTRACT

It is observed that information security auditors and experts experience a number of problems while accessing and working on information security standards. Some of these problems emanated from inaccessibility of security standards from a single point in an easy way; not being able to quickly compare and analyze standards with one another and from previous versions, and difficulties in deciding which standard should be used.

This thesis focuses on the development and implementation of a search tool for information security management systems (ISMS) standards by using open source software development platforms.

ISMS standards can be loaded to a database by using the search tool. This results in ISMS experts and auditors being able to reach the desired security standards easily at anytime and anywhere with just an internet connection. Users can search keywords within the standards and at the end of the search process, results are listed on a single page with the number of the title of the relevant standards. Users can also effortlessly see how often the searched keywords are included in each title. On the result page a chart is generated that displays the frequency of the keyword based on standards. This provides users with the ability to compare standards with one another.

The development of this tool has been based on ISMS standards, which is aimed at easing the use of, accessing and working with these standards. In this thesis, a case study of the tool was implemented successfully by using the ISO 27000 family of standards.

**Keywords:** Information Security Management Systems Standards, Information Security Management System Search Tool, ISMS, ISO/IEC 27001:2013.

# BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ İÇİN BİR ARAMA ARACI GELİŞTİRİLMESİ

## ÖZET

Bilgi güvenliği denetçilerinin ve uzmanlarının bilgi güvenliği standartlarına erişirken ve bunların üzerinde çalışırken bir takım problemle karşılaştıkları gözlenmiştir. Bu problemlerden bazıları; standartlara tek bir noktadan kolay bir şekilde erişilememesi, standartların bir birleriyle ve önceki sürümleriyle hızlı bir şekilde karşılaştırıp analiz edilememesi ve hangi standardın kuruma uygulanması gerektiğine karar vermede yaşanan zorluklardır.

Bu tez çalışmasında, Bilgi Güvenliği Yönetim Sistemleri (BGYS) standartları için açık kaynak yazılım geliştirme platformları kullanarak bir arama aracı geliştirilip uygulanması amaçlanmıştır.

Bu arama aracı sayesinde BGYS standartları bir veri tabanına yüklenebilmektedir. Böylece BGYS denetçileri ve uzmanları standartlara istediği zaman ve istediği yerde kolayca erişebilmektedir. Ayrıca, kullanıcılar standartlar içinde anahtar kelime aratabilmekte; arama işlemi ile çıkan sonuçlar, ilgili standardın başlık numarası ile beraber tek bir sayfada listelenmektedir. Kullanıcı anahtar kelimenin hangi başlıklar altında ve hangi yoğunlukta kullanıldığını kolayca görebilmektedir. Ayrıca anahtar kelimenin standart bazında kullanım sıklığını gösterir bir grafik sunularak standartları kıyaslamaya imkânı da tanınmıştır.

Bilgi Güvenliği Yönetim Sistemi standartları temel alınarak geliştirilen bu araç ile amaçlanan bilgi güvenliği standartlarına erişimi ve standartlar üzerinde çalışmayı kolaylaştırmaktır. ISO/IEC 27000 standart ailesi kullanılarak yapılan örnek bir çalışma ile aracın uygulaması başarı bir şekilde gerçekleştirilmiştir.

**Anahtar Sözcükler:** Bilgi Güvenliği Yönetim Sistemi Standartları, Bilgi Güvenliği Yönetim Sistemi Arama Aracı, BGYS, ISO/IEC 27001:2013.



# CONTENTS

M.Sc. THESIS EXAMINATION RESULT FORM .....	ii
ETİK BEYAN.....	iii
ACKNOWLEDGEMENTS.....	iv
ABSTRACT .....	v
ÖZET.....	vi
CONTENTS.....	vii
LIST OF ABBREVIATIONS AND ACRONYMS .....	x
LIST OF FIGURES .....	xi
LIST OF TABLES .....	xiv
CHAPTER 1 INTRODUCTION .....	1
1.1 Background.....	1
1.2 Problem .....	3
1.3 Objective.....	4
1.4 Related Work.....	4
1.5 Thesis Structure.....	6
CHAPTER 2 BASIC CONCEPTS OF INFORMATION SECURITY .....	7
2.1 Information Security Concepts .....	7
2.2 Information Security Management Systems (ISMS) .....	10
CHAPTER 3 IT RELATED STANDARDS .....	12
3.1 BSI Standard 100 (IT-Grundschutz).....	12
3.2 COBIT .....	14
3.3 ITIL.....	17
3.4 NIST Standards .....	19
3.5 OCTAVE.....	21
3.6 O-ISM3 .....	23
3.7 PCI DSS.....	24

<b>CHAPTER 4 ISO 27000 Family of Standards .....</b>	<b>26</b>
<b>4.1 ISO/IEC 27000 .....</b>	<b>28</b>
<b>4.2 ISO/IEC 27001 .....</b>	<b>28</b>
<b>4.2.1 History of the Standard .....</b>	<b>29</b>
<b>4.2.2 Plan-Do-Check-Act Model (PDCA) .....</b>	<b>29</b>
<b>4.3 ISO/IEC 27002 .....</b>	<b>31</b>
<b>4.4 ISO/IEC 27003 .....</b>	<b>32</b>
<b>4.5 ISO/IEC 27004 .....</b>	<b>32</b>
<b>4.6 ISO/IEC 27005 .....</b>	<b>33</b>
<b>4.7 ISO/IEC 27006 .....</b>	<b>34</b>
<b>CHAPTER 5 DEVELOPMENT TOOLS AND ENVIRONMENTS .....</b>	<b>36</b>
<b>5.1 Concepts and Advantages of Open Source .....</b>	<b>36</b>
<b>5.2 Web Based Applications .....</b>	<b>37</b>
<b>5.3 PHP .....</b>	<b>38</b>
<b>5.4 MySQL .....</b>	<b>39</b>
<b>5.5 Apache HTTP Server .....</b>	<b>39</b>
<b>5.6 XAMPP .....</b>	<b>40</b>
<b>5.7 Notepad++ .....</b>	<b>40</b>
<b>5.8 StarUML .....</b>	<b>40</b>
<b>5.9 MySQL Workbench .....</b>	<b>40</b>
<b>CHAPTER 6 IMPLEMENTATION .....</b>	<b>42</b>
<b>6.1 Introduction .....</b>	<b>42</b>
<b>6.2 Software Architecture .....</b>	<b>42</b>
<b>6.3 Database Design .....</b>	<b>45</b>
<b>6.4 Software Design .....</b>	<b>48</b>
<b>6.5 Administration Panel .....</b>	<b>48</b>
<b>6.5.1 Authentication Control .....</b>	<b>49</b>
<b>6.5.2 Administration Panel Main Page .....</b>	<b>50</b>
<b>6.5.3 Source Management .....</b>	<b>51</b>
<b>6.5.3.1 Creating New Source Profile .....</b>	<b>52</b>

6.5.3.2 View/Edit Source Profile.....	56
6.5.3.3 Block and Unblock Source Profile .....	59
6.5.3.4 Delete, Recover and Destroy Source Profile.....	61
6.5.4 Content Management .....	64
6.5.4.1 Adding New Content .....	67
6.5.4.2 View/Edit Content .....	69
6.5.4.3 Remove Content.....	70
6.5.5 User Management.....	72
6.5.5.1 Adding New User .....	73
6.5.5.2 View/Edit User .....	75
6.5.5.3 Remove User.....	76
6.5.6 Word Counter .....	78
6.6 End-User Panel .....	82
6.6.1 End-User Login Page.....	82
6.6.2 User Main Page .....	83
6.6.3 Search Query.....	84
6.6.4 Search Result.....	86
6.6.5 Keyword Index.....	89
CHAPTER 7 FUTURE WORK AND CONCLUSION.....	91
7.1 Future Work .....	91
7.2 Conclusion.....	92
REFERENCES.....	94
RESUME.....	97

## **LIST OF ABBREVIATIONS AND ACRONYMS**

BCP	: Business Continuity Planning
BS	: British Standard
BSI	: British Standard Institute
BSI	: German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
DIS	: Draft International Standard
CIDSS	: Common Intrusion Detection Signatures Standard
CISO	: Chief Information Security Officer
COBIT	: The Control Objectives for Information and Related Technology
ER Model	: Entity-Relationship Model
GUI	: Graphical User Interface
HTML	: Hyper Text Markup Language
HTTP	: Hyper-Text Transfer Protocol
HM	: Her Majesty's (Government), Government of the United Kingdom
ISMS	: Information Security Management System
ISO	: The International Organization for Standardization
IEC	: The International Electrotechnical Commission
IT	: Information Technology
JTC	: The Joint Technical Committee
MDA	: Model Driven Architecture
NIST	: National Institute of Standards and Technology
PDCA	: Plan-Do-Check-Act
PHP	: Hypertext Preprocessor
RDBMS	: Relational Database Management Systems
SSL/TLS	: Transport Layer Security/ Secure Sockets Layer
SOA	: Statement of Applicability
TR	: Technical Report
UK	: United Kingdom
UML	: Unified Modeling Language

## LIST OF FIGURES

<b>Figure 2.1</b> CIA triad illustration .....	8
<b>Figure 3.1</b> Overview of BSI publications on ISMS .....	13
<b>Figure 3.2</b> COBIT evolution of scope .....	15
<b>Figure 3.3</b> IT governance focus areas .....	16
<b>Figure 3.4</b> ITIL components.....	19
<b>Figure 4.1</b> The relationship of ISO 27000 family of standards.....	26
<b>Figure 4.2</b> PDCA cyclic model .....	31
<b>Figure 4.3</b> Information security risk management processes .....	34
<b>Figure 5.1</b> Server side programming schema.....	38
<b>Figure 6.1</b> The search tool application scenario.....	44
<b>Figure 6.2</b> Layered software architecture.....	45
<b>Figure 6.3</b> Database design for the ISMS search tool .....	46
<b>Figure 6.4</b> E-R diagram for the ISMS search tool.....	47
<b>Figure 6.5</b> Activity diagram for authentication.....	49
<b>Figure 6.6</b> Administration panel login page.....	50
<b>Figure 6.7</b> Administration panel main page .....	51
<b>Figure 6.8</b> Source management main page .....	52
<b>Figure 6.9</b> Activity diagram for creating a new source.....	53
<b>Figure 6.10</b> Create new source button.....	54
<b>Figure 6.11</b> Form for adding a new source .....	55
<b>Figure 6.12</b> A notification after adding a new source .....	56
<b>Figure 6.13</b> Activity diagram for view/edit source processes.....	57
<b>Figure 6.14</b> Editing a source .....	58
<b>Figure 6.15</b> Form for view/edit a source .....	58

<b>Figure 6.16</b>	A notification after editing a source .....	59
<b>Figure 6.17</b>	Block / unblock source .....	60
<b>Figure 6.18</b>	A notification after activating a source.....	60
<b>Figure 6.19</b>	Activity diagram for block/unblock source operations.....	61
<b>Figure 6.20</b>	A notification after deleting a source.....	62
<b>Figure 6.21</b>	Notification message after restore a source .....	62
<b>Figure 6.22</b>	Warning message before destroy a source.....	63
<b>Figure 6.23</b>	Activity diagram for source management processes .....	64
<b>Figure 6.24</b>	Content management main page: list of source .....	65
<b>Figure 6.25</b>	Selecting a source .....	65
<b>Figure 6.26</b>	Content list for a source .....	66
<b>Figure 6.27</b>	Activity diagram for content management processes .....	67
<b>Figure 6.28</b>	Add new content button.....	68
<b>Figure 6.29</b>	New content form .....	68
<b>Figure 6.30</b>	Selecting a content to edit.....	69
<b>Figure 6.31</b>	Content view/edit form .....	70
<b>Figure 6.32</b>	Deleting a content .....	71
<b>Figure 6.33</b>	Content deletion confirmation message.....	71
<b>Figure 6.34</b>	User management screen .....	72
<b>Figure 6.35</b>	Activity diagram for user management processes .....	73
<b>Figure 6.36</b>	Create new user button .....	74
<b>Figure 6.37</b>	New user form .....	74
<b>Figure 6.38</b>	Form validation.....	75
<b>Figure 6.39</b>	User profile view/edit form .....	76
<b>Figure 6.40</b>	User deletion .....	77

<b>Figure 6.41</b> Caution message before deleting a user.....	77
<b>Figure 6.42</b> A notification after deleting a user .....	78
<b>Figure 6.43</b> List of standard in word counter page .....	79
<b>Figure 6.44</b> Word counter warning message.....	80
<b>Figure 6.45</b> Activity diagram for word counter .....	81
<b>Figure 6.46</b> Activity diagram for end-user panel processes.....	82
<b>Figure 6.47</b> End-user login page .....	83
<b>Figure 6.48</b> End-user main page .....	84
<b>Figure 6.49</b> Search result page .....	87
<b>Figure 6.50</b> Keyword repetition table .....	88
<b>Figure 6.51</b> Keyword frequency graphic.....	88
<b>Figure 6.52</b> Content page .....	89
<b>Figure 6.53</b> Keyword index page .....	90

## **LIST OF TABLES**

Table 2.1 A sample CIA triad table for risks, controls and primary focus. ....	10
Table 3.1 Specifications in the Federal Information Security Management Act.....	20
Table 4.1 PDCA description .....	30
Table 6.1 A sample query .....	85





# CHAPTER 1

## INTRODUCTION

### 1.1 Background

Information is a vital resource for all organizations such as companies, universities, non-profit organizations and states because information provides superiority, prestige, success and competitive power.

Protecting information is important because information also provides opportunities and unforeseen future advantages. Maximizing income and profit derived from investments, sustaining trade opportunities and the prestige of a company, country or any organization generally depends on solid protection of its information. When an organization fails to protect it, information may be stolen, damaged, or it may become unusable or it may even pass into unwanted parties hands. In this sense, information is a worth and the act of protecting is a serious matter. At this point, “information security” as a lexicon is emerging as a new pursuant phrase to the importance of information.

Information security is the protection of any type of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction of data. Defining, implementing, maintaining and continually improving information security is a basic and an essential requirement for all organizations. Information security protects commercial image, maintains competitive advantages, sustains profitability, and fulfills legal obligations.

Information security does not involve a single type of technology; more precisely it is a strategy which involves processes, tools and policies necessary to prevent, detect, and refuse threats to digital and non-digital information. Processes and policies typically involve both physical and digital security measures to protect data from unauthorized access, use, replication or destruction. Information security management can include everything from physically locking your drawer to encrypting digital data.

On the other hand, a variety of information distribution channels, the prevalence of information technology tools and more complex mesh computer networks makes information more vulnerable to external threats. This also complicates and makes it difficult to protect this information. Organizations need a good solid framework coupled with a systematic approach to ensure realization of information security in an effective way. Likewise, it is not only a sufficient motivation for organizations to protect their information, but customers and other organizations in the business relationship with the organization are required to prove whether or not the information they provide is safe or not.

Organizations need an information security management system to ensure information security has been designed for a robust framework in order to fulfill legal obligations and to give assurance to customers and stakeholders about their information being secure.

Information Security Management System (ISMS) has been defined to manage the sensitive information of the organization, thus represents a systematic approach to run in order to maintain the information in confidence. It includes people, processes and IT systems by applying a risk management process. It can help small, medium and large businesses in any sector keep information assets secure [1].

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art [2]. ISO (the International Organization for Standardization) IEC (the International Electrotechnical Commission) and Subcommittee SC 27 has developed international management systems standards for information security, called as ISO/IEC 27000, otherwise known as the ISMS family of standards.

ISO indicates that at the beginning of the ISO 27000:2014 standard; through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets including financial information, intellectual property, and employee details, or information entrusted to

them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information [2].

Information security auditors and experts manage information security by using some standards. The ISO 27000 family of standards also helps organizations keep information assets secure. This family consist of many standards and the ISO/IEC 27001 is the best-known standard in the family providing requirements for an ISMS.

## **1.2 Problem**

Adaptation of information security has its challenges. There is a need for a systematic and a pre-defined approach to deal with them. Sustainability of information security is another challenge for organizations which requires continuous control and development. To overcome these challenges many information security management systems have been established.

There are many standards to guide information security management such as ISO/IEC 27001, BSI-100, CMMI, COBIT, COSO, ITIL, NIST SP 800-53, OCTAVE, O-ISM3, PCIDSS, PMMM and SOA. Some of these standards may not be suitable or sufficient to ensure information security for all type of organizations and some may be. In general, ISO/IEC 27001, BSI-100, NIST SP 800-53, OCTAVE, O-ISM3 and PCIDSS are internationally preferred standards which provide details specific to information security. However, ISO/IEC 27001 is the most popular out of them due to being applicable to organizations of all types and sizes.

Information security auditors and experts experience a number of problems while working on ISMS standards. Accessing standards is one of the main problems. Reason being there are many institutions which publish families of standards which naturally means a huge number of individual standards related with information security. Even if ISO/IEC 27001 is the preferred standard, there may be a lot more standards under the ISO/IEC 27000 family that need to be worked with.

In the classical method, information security professionals use hardcopy or digital softcopy but usually it is not useful for them. When they want to access specific content it becomes a tedious process similar to a treasure hunt.

Second problem is comparing ISMS standards with one another and comparing institutions. It is difficult to make comparisons between them to understand which standard suits which organization.

Another issue is adapting to new releases of standards. For instance, ISO tend to update ISMS standards very often so information security auditors and professionals have difficulties in adapting to new releases, so they need to compare them.

### **1.3 Objective**

The purposes of this thesis are listed below,

- i. To develop a web based ISMS search tool to make working on ISMS standards easier. By using this search tool ISMS standards can be loaded to a database, thus ISMS experts and auditors can reach the standards easily at anytime and anywhere so long they have an Internet connection.
- ii. To provide a platform-independent tool with a simple user interface for users to search for keywords within the ISMS standards. Search results are listed on a single page with the relevant standard. Users can also easily see how often a keyword is passed in each title and context.
- iii. To generate a chart on a result page which shows the frequency of keywords on the basis of standards. It also allows users to compare standards with other standards and previous versions.

### **1.4 Related Work**

There are many tools for ISMS. Many of them commercial and provide fully integrated solutions. Some of them are as follows;

- Eremba, is an open-source, community oriented web-application that helps Technology, IT Security, Compliance and Audit professionals with the analysis, management and reporting of Security Governance. This tool provides fully integrated solution for setup an ISMS to an organization [3].

- Verinice is a tool for managing information security and supports user in their daily work as a CISO or IT Security Officer. By using Verinice users are able to do followings. a) Establishing, maintaining and improving an ISMS based on ISO 27001, BSI IT Baseline Protection, IDW PS 330 or other standards. b) Assuring the compliance with standards such as ISO 27002, BSI IT-Baseline Security, VDA IS-Assessments and many more. c) Performing risk analysis based on ISO 27005. d) Auditing, document management, report [4].
- SecureAware is an all-in-one ISMS tool that manages policies, IT controls and risk information that are in disparate locations throughout the enterprise. It creates continuous compliance by automating risk management and continuous improvement processes in an ISMS as defined in the ISO 27001 standard. SecureAware ISMS tool helps organization spend less time on IT governance, risk and compliance management while allowing to optimize information security management and achieve continuous compliance with security standards and regulations [5].
- ISMart is a software to manage all processes included in the organizational information security system. It provides tools that allow ISMS to be installed and sustained in compliance with the ISO/IEC 27001, audited and directed in compliance with the ISO/IEC 27002. Basically, ISMart contains functional modules including risk management, assessment-evaluation, incident management, internal audit, work flow and document management [6].

Automation tools are generally useful for organizations for example, using spreadsheets for assessing risks can be a problem when users have to merge results from different departments; or if organization has many different recovery plans and want to change the same detail in each of them, using a tool is probably much easier.

However, using such automation tools for organizations can be very expensive to integrate and training may take too much time. Also any of these tools do not include ISMS standards.

In this study, a single and simple search tool for ISMS standards is proposed. This tool provides advanced search options and keyword analysis for users working with ISMS standards.

## **1.5 Thesis Structure**

This thesis consists of 7 chapters.

CHAPTER 1, contains background information, problem formulation, objectives and thesis structure. Under the title of background, a brief definition of information security and information security management system are given.

CHAPTER 2, provides literature review on information security and management systems. In this section some main concepts of information security are explained.

CHAPTER 3, includes information about the best ISMS and standards.

CHAPTER 4, the globally preferred ISO 27000 family of standards are described more comprehensively.

CHAPTER 5, contains details about development tools and environment used during the development phase of ISMS search tool.

CHAPTER 6, explains implementation details and outcomes of the ISMS search tool. A sample study is also included in this chapter.

CHAPTER 7, covers possible future work and the conclusion.

# CHAPTER 2

## BASIC CONCEPTS OF INFORMATION SECURITY

In this chapter, the basic concepts of information security and the most preferred information security related standards are explained.

### **2.1 Information Security Concepts**

The term of information security evokes security in information technology in minds. From this wrong perception that are likely to be, most organizations only attach importance to technical measures to protect themselves from attack and breaches. But in fact, the term “information security” covers all of the thing where the information is located so information security is not only means computer security but also means protecting any form of information.

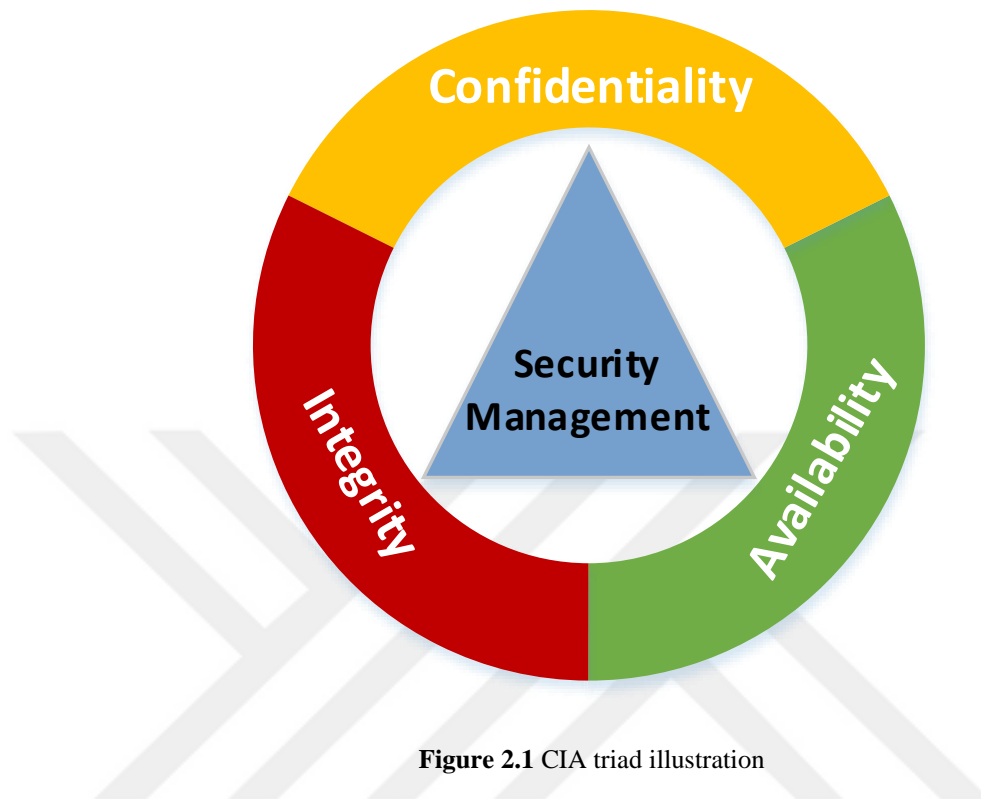
For example, a customer information that was written on a paper, a printed document which contains private graphics and a network topology that hung on wall. Each one of them is an information and outside the forms of information technology. For this reason, when the word of “information” is stated it must be addressed within this scope.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

If the term of “information security” stated technically, in the US Code it is expressed as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability [7] . Congruently, according to ISO/IEC 27000:2014; information security is preservation of confidentiality, integrity and availability of information [2].

At this point, the following question may come to mind: “What is confidentiality, integrity and availability?” It is also known as the CIA abbreviation formed from the

initial letters of the words. The CIA triad illustrated in Figure 2.1, which is used to identify problem areas and necessary solutions for information security.



**Figure 2.1** CIA triad illustration

The short description of confidentiality, integrity and availability are discussed below.

1. Confidentiality. According to ISO confidentiality defined as property that information is not made available or disclosed to unauthorized individuals, entities, or processes [2]. For example, an email with sensitive information. No one wants personal email to be read by anyone else so communication environment must provide confidentiality. Encryption is a good example and solution to provide the confidentiality because it ensures that only the right people (who has the right key) can read the information. Encryption is widespread in today and can be found in almost every major protocol in use. A featured example of encryption is SSL/TLS, a security protocol for communications over the internet that has been used with a large number of internet protocols to ensure security.



2. Integrity refers accuracy and completeness of information [2]. It also means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. In lifecycle, information must not be altered by unauthorized parties and must not be changed erroneously or accidentally by authorized users. In addition, sometimes data is affected non-human-caused or unintended events. To avoid of them, detect any changes and provide integrity some solution methods may be used.
  
3. Availability is being information accessible and usable upon demand by an authorized entity [2]. The information must be available and reachable by authorized users when it is needed. The computing systems, communication channels and other environments must be functioning correctly to prevent service disruption and remain availability. Ensuring availability also involves preventing attacks to the target systems essentially the aim of service interruption.

A sample risks, controls and primary focus table in terms of CIA triad is given in Table 2.1.

**Table 2.1** A sample CIA triad table for risks, controls and primary focus.

<b>CIA</b>	<b>Risks</b>	<b>Controls</b>	<b>Primary Focus</b>
<b>Confidentiality</b>	Loss of privacy Unauthorized access to information. Identity theft	Encryption Authentication Access controls	Information Security
<b>Integrity</b>	Information is no longer reliable or accurate. Fraud	Maker/Checker Quality assurance Audit logs	Operational Controls
<b>Availability</b>	Business disruption, Loss of customer confidence. Loss of revenue	BCP <sup>1</sup> Plans and tests Back-up storage Sufficient capacity	Business Continuity Planning

## 2.2 Information Security Management Systems (ISMS)

Accomplishment of information security necessitates the management of risk and threats related with all forms of information within organization. This should be done by using robust framework which has well defined processes, policies and procedure. This framework should also include organizational structures, planning activities, responsibilities, practices and resources. This framework need to be established, implemented, monitored, reviewed and improved consummately to fulfill the security objectives.

In brief, there is a need to look at information security from a holistic perspective, and to have an information security management methodology to protect information systematically. This is where the need for Information Security Management Systems (ISMS) comes in.

According to ISO, an ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives [2].

<sup>1</sup> BCP: Business Continuity Planning is the process of creating systems of prevention and recovery to deal with potential threats to a company.

The ISO/IEC 27000 family of standards is the globally most preferred one. However, there are many standards and procedure involving with information security or risk management.

Some of the most used information security related or IT related standards published outside of ISO/IEC are described in CHAPTER 3. In addition, ISO/IEC 27000 family of standards will be examined more comprehensively in CHAPTER 4.



# CHAPTER 3

## IT RELATED STANDARDS

There are many standards and procedure that can be used for information security management as well as the ISO 27000 standards. In this chapter some of the best known information security and IT related standards and procedure are explained. Standards and procedures are described in alphabetical order.

### **3.1 BSI Standard 100 (IT-Grundschutz)**

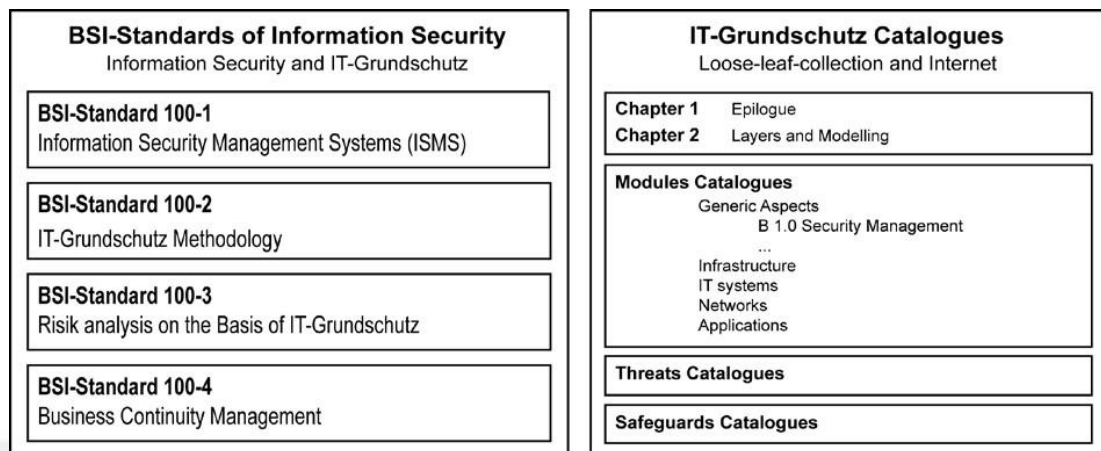
Bundesamt für Sicherheit in der Informationstechnik (BSI) is the German Federal Office for Information Security. The BSI is known for IT baseline protection manual which is named as ITGrundschutz. This manual guides an ISMS including a governance structure and information security controls. It is gradually being aligned with ISO/IEC 27000 and it has been divided into methods and controls which is like ISO/IEC 27002.

The BSI Standards contain recommendations by the German Federal Office for Information Security (BSI) on methods, processes, procedures, approaches and measures relating to information security. For this, the BSI addresses issues that are of fundamental importance for information security in public authorities and companies and for which appropriate, practical, national or international approaches have been established [8].

Although, IT-Grundschutz is similar ISO/IEC 27000 in some ways, it has some differences. The main difference is IT-Grundschutz offers a practical common security reference line rather than ISO27000 offers a risk-based and theoretical approach. On the other hand, BSI Standards are also used to depict proven approaches to cooperation. BSI Standards can be quoted, and this will contribute to establishing uniform specialist terms [8].

BSI series of standards for information security consists of five main components. These are BSI-Standard 100-1, BSI-Standard 100-2, BSI Standard 100-3, BSI

Standard 100-4 and IT-Grundschatz Catalogues. Overview of BSI publications on Information Security management is given in Figure 3.1.



**Figure 3.1** Overview of BSI publications on ISMS

The BSI 100-1 fully name is “BSI-Standard 100-1: Information Security Management Systems” defines the general requirements of an ISMS. It is fully compatible with the ISO 27001 standard and also takes the recommendations of the ISO 27001 and 27002 standards into consideration. It provides readers with an easy to understand and systematic instruction manual irrespective of which method they want to use to implement the requirements [9].

Second, “BSI-Standard 100-2: IT-Grundschatz Methodology” goes into great detail on how a policy for information security can be developed in practice, how appropriate information security safeguards can be selected and what should be watched out for when implementing the policy of information security. It also in detail answers the question of how to maintain and improve information security during routine operation [9].

The IT-Grundschatz Methodology is almost similar to ISO/IEC 27001 because it is essentially about governance of information security. It explains practically how a management system for information security can be established, implemented and maintained. It provides useful examples based on a suppositional goernance to show specific steps of the approach. It also references to PDCA, and run ISMS implementation steps.

Third is “BSI Standard 100-3: Risk analysis based on IT-Grundschutz”. It is a bit similar to ISO/IEC 27005. In contrast to ISO27000 family of standards, the IT-Grundschutz baseline approach uses the catalogues to specify security controls. This document outlines a methodology for determining, for specific targets and for as little effort as possible, whether and in what respect there is any need to take action over and above the IT-Grundschutz in order to contain risks for information processing [10].

Fourth one is “BSI Standard 100-4: Business Continuity Management”. The BSI Standard 100-4 points out a systematic way to develop, establish and maintain an agency-wide or company-wide internal business continuity management system.

The goal of business continuity management is to ensure that important business processes are only interrupted temporarily or not interrupted at all, even in critical situations. To ensure the operability, and therefore the survival, of a company or government agency, suitable preventive measures must be taken to increase the robustness and reliability of the business processes as well as to enable a quick and targeted reaction in case of an emergency or a crisis [8].

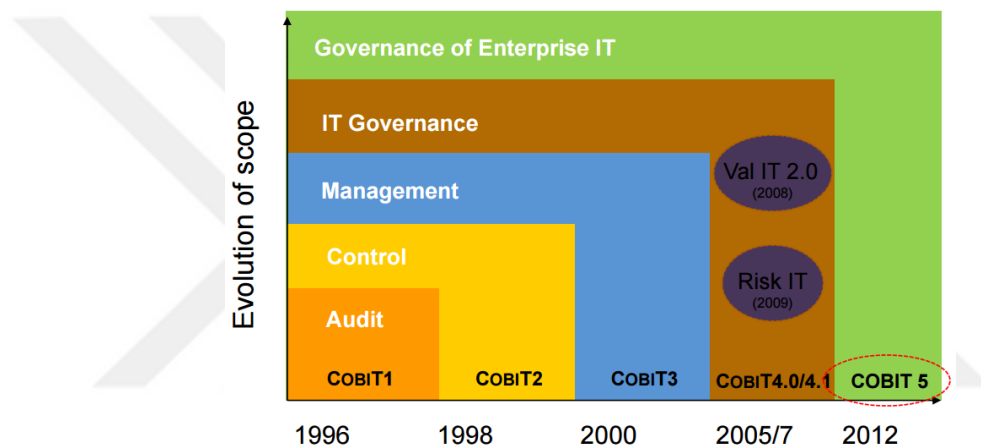
The last one is IT-Grundschutz Catalogues. According to German Federal Office of Information Security, one of the most important objectives of IT-Grundschutz is to reduce the expense of the information security process by offering reusable bundles of familiar procedures to improve information security. In this manner, the IT-Grundschutz Catalogues contain standard threats and security safeguards for typical business processes and IT systems which can be used in organization, if necessary. The IT-Grundschutz Catalogues not only explain what has to be done, they also provide very specific information as to what implementation (even at a technical level) may look like [8].

### **3.2 COBIT**

COBIT is a framework for developing, implementing, monitoring and improving information technology (IT) governance and management practices. The COBIT framework is developed by the IT Governance Institute

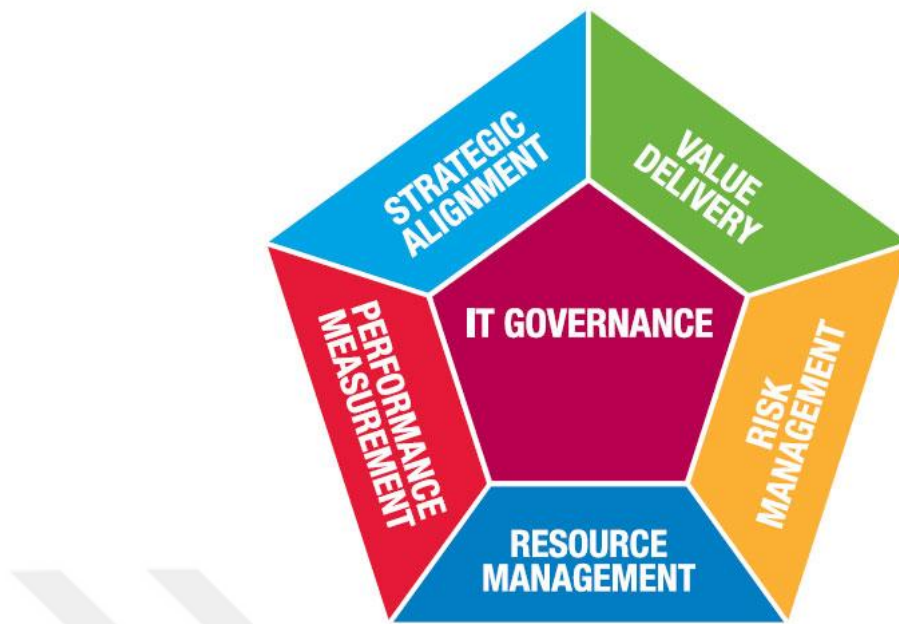
and the Information Systems Audit and Control Association (ISACA). The main idea of the COBIT provides a common culture for goals, objectives and results. Internationally recognized COBIT helping IT professionals and enterprise leaders achieve their IT Governance liabilities.

The first and original version, published in 1996, generally focused on auditing. The latest version, published in 2012, emphasizes the value that information governance can provide to a business' success. It also provides quite a bit of advice about enterprise risk management. The evolution of scope of COBIT is given in Figure 3.2 [11].



**Figure 3.2** COBIT evolution of scope

Control Objectives for Information and related Technology (COBIT®) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimize IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong [12]. The IT governance focus areas are given in Figure 3.3.



**Figure 3.3** IT governance focus areas

Strategic alignment focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations [12].

Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT [12].

Resource management is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure [12].

Risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization [12].

Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery using, for



example, balanced score cards that translate strategy into action to achieve goals measurable beyond conventional accounting [12].

According to ISACA benefits of COBIT is given as follows [13].

1. Maintaining high-quality information to support business decisions
2. Achieving strategic goals and realize business benefits through the effective and innovative use of IT
3. Achieving operational excellence through reliable, efficient application of technology
4. Maintaining IT-related risk at an acceptable level
5. Optimizing the cost of IT services and technology
6. Supporting compliance with relevant laws, regulations, contractual agreements and policies

### **3.3 ITIL**

ITIL is a best practice framework that has been drawn from both the public and private sectors internationally. It describes how IT resources should be organized to deliver business value, documenting the processes, functions and roles of IT Service Management (ITSM).

The ITIL concept emerged in the 1980s, when the British government determined that the level of IT service quality provided to them was not sufficient. The Central Computer and Telecommunications Agency (CCTA), now called the Office of Government Commerce (OGC), was tasked with developing a framework for efficient and financially responsible use of IT resources within the British government and the private sector. The concepts within ITIL support information technology services delivery organizations with the planning of consistent, documented, and repeatable or customized processes that improve service delivery to the business [14].

The ITIL framework consists of the following IT processes: Service Support (Service Desk, Incident Management, Problem Management, Change Management, Configuration Management, and Release Management) and Services Delivery (Service Level Management, Capacity Management, Availability Management, Financial Management and IT Service Continuity Management) [14].

The ITIL has seven components described as follows [15]. The components are illustrated in Figure 3.4:

1. Service Support: This ensures appropriate services are in place to support business functions. Service Support includes Configuration Management, Service Desk, Incident Management, Problem Management, Change Management, and Release Management.
2. Service Delivery: This ensures that business functions receive adequate services to accomplish goals. Service Delivery includes Availability Management, Capacity Management, IT Services Continuity Management, IT Services Financial Management, and Service Level Management.
3. Security Management: This ensures that Security Management requirements are implemented as outlined in the Service Level Agreement. Security Management is the only process included in this section.
4. Application Management: This ensures that the appropriate software development life cycle is followed. Application Management includes Software Lifecycle Support and Testing of IT Services.
5. ICT Infrastructure Management: This section covers Network Service Management, Operations Management, Management of Local Processors, Computer Installation and Acceptance, and Systems Management.
6. Business Perspective: This section includes Business Continuity Management, Partnerships and Outsourcing, Surviving Change and Transformation of Business Practices through Change, and Understanding and Improving.

7. Planning to Implement Service Management: This explains how to implement ITIL and what benefits organizations may gain from it. This section covers Continuous Process Improvement.

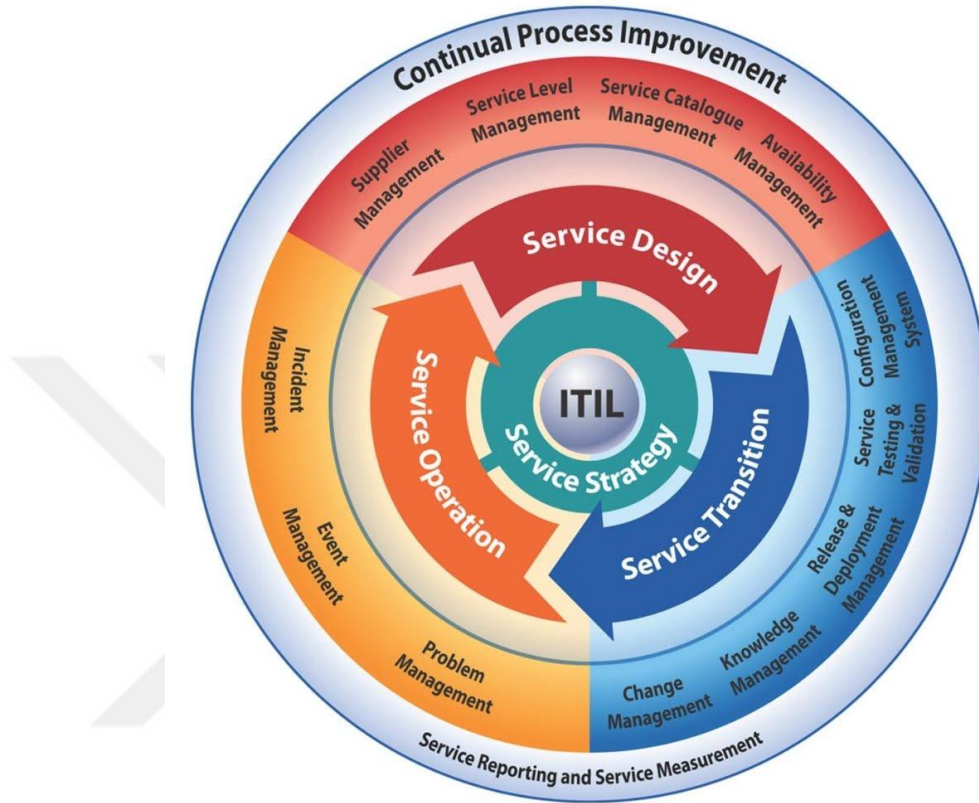


Figure 3.4 ITIL components

### 3.4 NIST Standards

The US National Institute of Standards and Technology (NIST) is well-known for producing well-written, clear and comprehensive technical standards. Unlike ISO 27000 family of standards they are free of charge. NIST Special Publications 800 series of standards are related with information security.

According to NIST, NIST Special Publication 800-53 provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other

organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors [16].

The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs [16].

The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation [16].

Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability) [16].

NIST has specified guidelines for implementing the US Federal Information Security Management Act (FISMA). This act aims to provide the following standards shown in Table 3.1.

**Table 3.1** Specifications in the Federal Information Security Management Act

<ul style="list-style-type: none"><li>• Standards for categorizing information and information systems by mission impact</li></ul>
<ul style="list-style-type: none"><li>• Standards for minimum security requirements for information and information systems</li></ul>
<ul style="list-style-type: none"><li>• Guidance for selecting appropriate security controls for information systems</li></ul>
<ul style="list-style-type: none"><li>• Guidance for assessing security controls in information systems and determining security control effectiveness</li></ul>
<ul style="list-style-type: none"><li>• Guidance for the security authorization of information systems</li></ul>
<ul style="list-style-type: none"><li>• Guidance for monitoring the security controls and the security authorization of information systems</li></ul>

### **3.5 OCTAVE**

OCTAVE was developed by CERT which stands for "Computer Emergency Readiness Team". CERT was formed by the US Defense Advanced Research Projects Agency (DARPA) in November 1988 after the Internet was assaulted in the Internet worm incident. Officially called the CERT Coordination Center, is located at Carnegie-Mellon University in Pittsburgh where it is part of the Networked Systems Survivability program in the Software Engineering Institute. It is a research and development center funded by federally in USA.

CERT is the Internet's official emergency team, focuses on security breach and denial-of-service incidents, providing alerts and incident-handling and avoidance guidelines in the USA. CERT also conducts an ongoing public awareness campaign and engages in research aimed at improving security systems. One of the primary goals of the CERT is to help organizations ensure that their information security activities are aligned with their organizational goals and objectives.

The OCTAVE method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) was created by CERT to help organizations perform information security risk assessments in context with the operational and strategic drivers that they rely on to meet their mission [17].

The OCTAVE method is an approach used to assess an organization's information security needs.

OCTAVE methods are self-directed, flexible, and evolved. Using OCTAVE, small teams across business units and IT work together to address the security needs of the organization. The method can be tailored to the organization's unique risk environment, security and resilience objectives, and skill level. OCTAVE moves an organization toward an operational risk-based view of security and addresses technology in a business context [17].

OCTAVE Original defines three stages:

Phase 1: Creating a threat profile for assets

Phase 2: Defining vulnerabilities

Phase 3: Developing a strategy

One of the versions named as OCTAVE Allegro focuses on information assets. An organization's important assets are identified and assessed based on the information assets to which they are connected. This process eliminates potential confusion about scope and reduces the possibility that extensive data gathering and analysis are performed for assets that are poorly defined, outside of the scope of the assessment, or in need of further decomposition [17].

OCTAVE Allegro can be performed in a workshop-style, collaborative setting, and is well suited for those who want to perform risk assessment without extensive organizational involvement, expertise, or input. OCTAVE Allegro consists of eight steps organized into four phases [17]:

1. Develop risk measurement criteria consistent with the organization's mission, goal objectives, and critical success factors.
2. Create a profile of each critical information asset that establishes clear boundaries for the asset, identifies its security requirements, and identifies all of its containers.
3. Identify threats to each information asset in the context of its containers.
4. Identify and analyze risks to information assets and begin to develop mitigation approaches.

The OCTAVE Allegro is documented in the SEI report *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. The report explains the design considerations and specifications for OCTAVE Allegro, which were all based on field experience [17].

### 3.6 O-ISM3

The Open Group for managing information security developed Open Information Security Management Maturity Model (O-ISM3).

The Open Group is a global vendor-neutral and technology-neutral consortium that enables the achievement of business objectives through IT standards. Its goal makes available access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group has 500 member organizations that involves all sectors of the IT community which are customers, systems and solutions suppliers, tool vendors, integrators and consultants, as well as academics and researchers [18].

The main purposes of Open Groups are to [18];

- Capture, understand and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

O-ISM3 is the Open Group framework for managing information security. It aims to ensure that security processes operate at a level consistent with business requirements. ISM3 is technology-neutral. It defines a comprehensive but manageable number of information security processes sufficient for the needs of most organizations, with the relevant security control(s) being identified within each process as an essential subset of that process. In this respect, it is fully compatible with the well-established ISO/IEC 27000:2009, COBIT, and ITIL standards in this field. Additionally, as well as complementing the TOGAF model for enterprise architecture, ISM3 defines operational metrics and their allowable variances [19].

ISM3 is designed with all kinds of organization in mind. In particular, businesses, nongovernmental organizations, and enterprises that are growing or outsourcing may find ISM3 attractive. In summary, ISM3 [19]:

- Provides a tool for creating ISMSs that are fully aligned with the business mission and compliance needs
- Applies to any organization regardless of size, context, and resources
- Enables organizations to prioritize and optimize their investment in information security
- Enables continuous improvement of ISMSs using metrics
- Enables metric-driven, verifiable outsourcing of security processes

### **3.7 PCI DSS**

In this 21<sup>st</sup> century, large numbers of financial transactions are carried out electronically. Electronic transactions are accelerating the process by facilitating access, expanding and diversifying. Today, a significant portion of the financial account transactions constitute such credit card owner data. This data is one of the most important targets most exposed to threats on electronic communications. However, the most important thing is that organizations are required to protect electronic transaction data yet.

In this context, the Payment Card Industry (PCI) Data Security Standard (DSS) is one of the information security standard defined by the Payment Card Industry (PCI) Security Standards Council (SSC). The standard was created to help industry organizations processes card payments and to prevent credit card fraud.

Besides, the PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and



service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks [20].



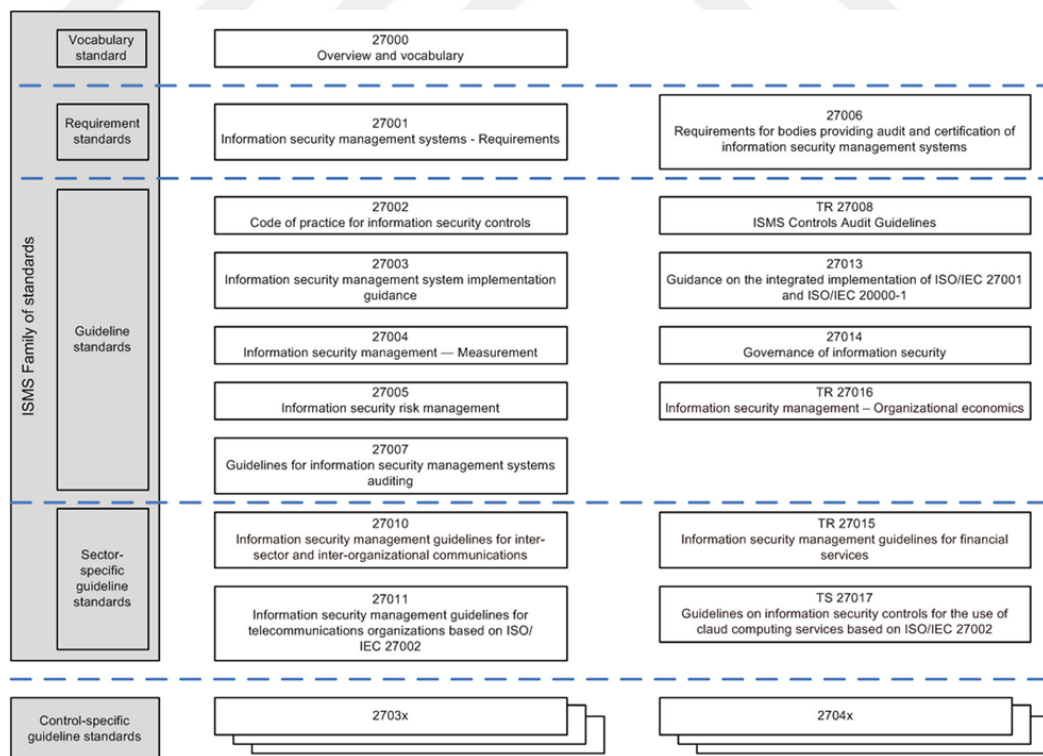
# CHAPTER 4

## ISO 27000 Family of Standards

In the previous chapter, general information was given about the IT standards which related to information security. In this chapter, an ISMS framework ISO 27000 family of standards will be described.

The ISMS family of standards consists of inter-related standards, already published or under development, and contains a number of significant structural components. These components are focused upon normative standards describing ISMS requirements (ISO/IEC 27001) and certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001. Other standards provide guidance for various aspects of an ISMS implementation, addressing a generic process, control related guidelines as well as sector-specific guidance [2].

Relationships between the standards of ISO 27000 series are illustrated in Figure 4.1.



**Figure 4.1** The relationship of ISO 27000 family of standards

It is aimed to help organizations to implement and maintain an ISMS by publishing the ISO 27000 family of standards. Standards of the family are named under the general title Information technology — Security techniques. Some of the certain members of ISO 27000 series are given below in numerical order [1]:

- a) ISO/IEC 27000, Information security management systems — Overview and vocabulary
- b) ISO/IEC 27001, Information security management systems — Requirements
- c) ISO/IEC 27002, Code of practice for information security controls
- d) ISO/IEC 27003, Information security management system implementation guidance
- e) ISO/IEC 27004, Information security management — Measurement
- f) ISO/IEC 27005, Information security risk management
- g) ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
- h) ISO/IEC 27007, Guidelines for information security management systems auditing
- i) ISO/IEC TR 27008, Guidelines for auditors on information security controls
- j) ISO/IEC 27009 (Under development), Sector-specific application of ISO/IEC 27001 Requirements
- k) ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications
- l) ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- m) ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

- n) ISO/IEC 27014, Governance of information security
- o) ISO/IEC TR 27015, Information security management guidelines for financial services
- p) ISO/IEC TR 27016, Information security management — Organizational economics

#### **4.1 ISO/IEC 27000**

ISO/IEC 27000 International Standard can be considered as introduction of ISO 27000 family of standards. It includes frequently used terms and definitions used in the ISO 27000 series. It also explains introduction and basic concepts of ISMS.

ISO/IEC 27000 provides definitions of other standards that members of ISO 27000 series to provide a quick view. There are four editions of ISO 27000. The last and updated one is ISO/IEC 27000:2016 which has been published in 15 February 2016.

The ISO 27000 family of standards helps organizations keep information assets secure. Using this family of standards help organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted to the organization by third parties [21].

The other common standards members of the ISO 27000 family are described below.

#### **4.2 ISO/IEC 27001**

The international standard of ISO/IEC 27001 is the best-known standard in the family. The official full name is “ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements”. It designed to ensure the selection of an adequate and proportionate security controls to protect information assets. This standard is usually applicable to all types of organizations which can be either private or public and big or small.

The main purpose of ISO IEC 27001 is to help organizations to establish and maintain an ISMS (Detailed information about ISMS was described in section 2.2).

ISO/IEC 27001 specifies requirements for ISMS. These requirements are related with establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS. Also, these requirements consist of seven sections in ISO/IEC 27001:2013 standard which are: Context, Leadership, Planning, Support, Operation, Evaluation and Improvement. According to ISO IEC 27001, organization fulfill every requirement to be able to claim that ISMS complies with this standard.

On the other hand, requirements provided in ISO/IEC 27001 including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS [2].

#### **4.2.1 History of the Standard**

ISO/IEC 27001 is derived from BS 7799 Part 2, published in 1999. BS 7799 Part 2 was revised by British Standard Institute (BSI) in 2002, it is clearly involving Plan-Do-Check-Act (PDCA) cyclic process concept, and was adopted by ISO/IEC as ISO/IEC 27001 in 2005. It was comprehensively revised in 2013 and bringing it compatible with the other ISO certified management systems standards. The 2013 edition does not compel PDCA approach. ISO/IEC 27001:2013 allows to use either PDCA or other approaches. But in practice, it can be deduced the PDCA cycle in the structure of ISO standard, namely, sections of ISO/IEC 27001:2013 can be divided into phase according to PDCA model as follows.

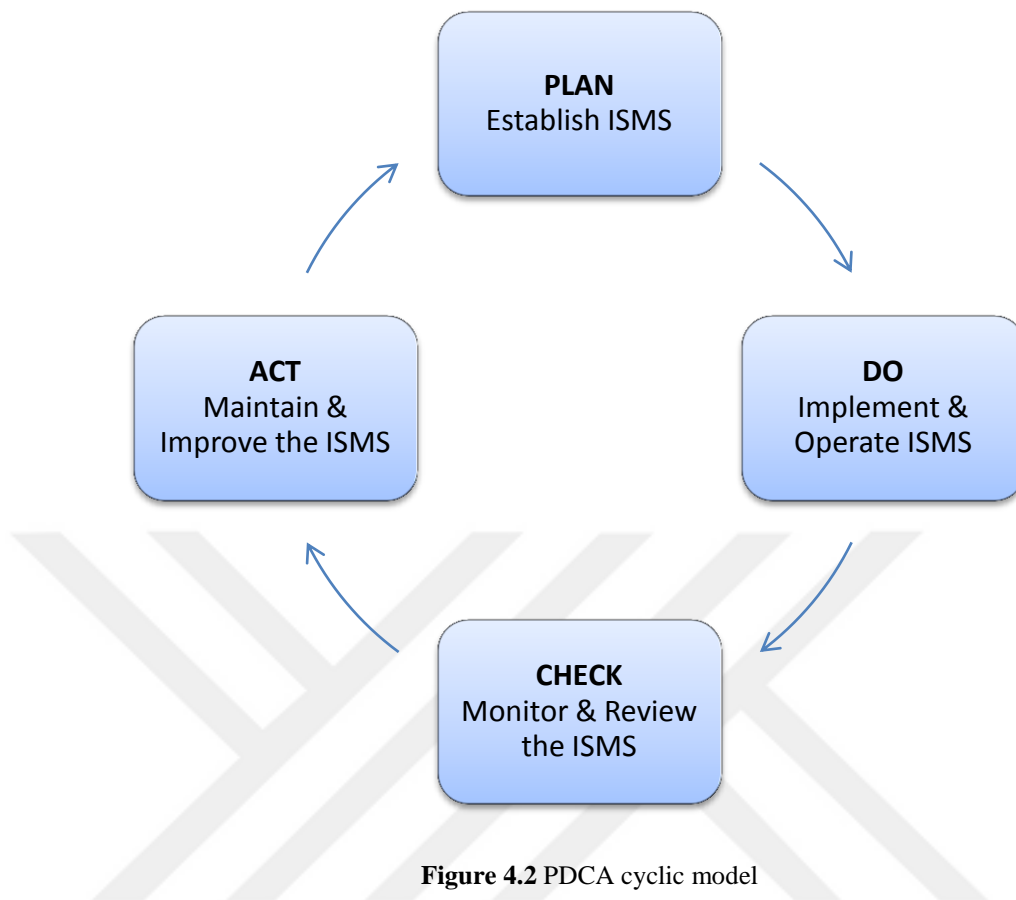
- Plan phase: Clauses 4 Context of the organization, 5 Leadership, 6 Planning, and 7 Support
- Do phase: Clause 8 Operations speaks about the
- Check Phase: Clause 9 Performance evaluation
- Act Phase: Clause 10 Improvement

#### **4.2.2 Plan-Do-Check-Act Model (PDCA)**

The description of PDCA is given in Table 4.1 and PDCA cyclic diagram is illustrated in Figure 4.2 [22].

**Table 4.1** PDCA description

<b>Plan</b> <b>(establish the ISMS)</b>	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.
<b>Do</b> <b>(implement and operate the ISMS)</b>	Implement and operate the ISMS policy, controls, processes and procedures.
<b>Check</b> <b>(monitor and review the ISMS)</b>	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
<b>Act</b> <b>(maintain and improve the ISMS)</b>	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.



**Figure 4.2** PDCA cyclic model

### **4.3 ISO/IEC 27002**

ISO/IEC 27002:2013 is an information security management standard. It defines a set of recommended information security controls. The official full name of the standard is “ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls”.

ISO/IEC 27002 is a popular, internationally-recognized standard of good practice for information security. Basically, ISO/IEC 27002:2013 is based on the BS 7799 standard and has a 30-year history.

This International Standard provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance when selecting and implementing controls for achieving information security. ISO/IEC 27002 provides guidance on the implementation of information security controls [2].

#### **4.4 ISO/IEC 27003**

ISO/IEC 27003 provides implementation guidance to help those implementing the ISO27000 family of standards, covering the management system aspects in particular. The official full name of this standard is “ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance”.

This standard has been established to lead to the initiation of ISO/IEC 27001 based ISMS. It explains the process of ISMS specification and design from beginning to the production of implementation plans. This processes also includes the preparation and planning activities.

ISO/IEC 27003 gives recommendations and explanations; it does not specify any requirements. This standard is intended to be used in conjunction with ISO/IEC 27001 and ISO/IEC 27002, but is not intended to modify and/or reduce the requirements specified in ISO/IEC 27001 or the recommendations provided in ISO/IEC 27002 [23].

The revised standard is at DIS (Draft International Standard) stage. It is scheduled to be published in the year 2016.

#### **4.5 ISO/IEC 27004**

ISO/IEC 27004:2009 defines measurements relating to information security management. These are commonly known as ‘security metrics’ in the profession. The official full name of this standard is “ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement”.

The standard is intended to help organizations measure, report on and hence systematically improve the effectiveness of ISMS.

It provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security



management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001. This would include policy, information security risk management, control objectives, controls, processes and procedures, and support the process of its revision, helping to determine whether any of the ISMS processes or controls need to be changed or improved [24].

The standard includes a little more detail in terms of measurement processes. It explains how to gather “base measures” and calculations method to produce “derived measures” by using aggregation and mathematical method. Also, the standard describes calculation methods and decision criteria to produce “indicators” used to manage information security policy. Deficiently, it does not offer detailed explanation to understand which measures or indicators might really be valuable and which is not.

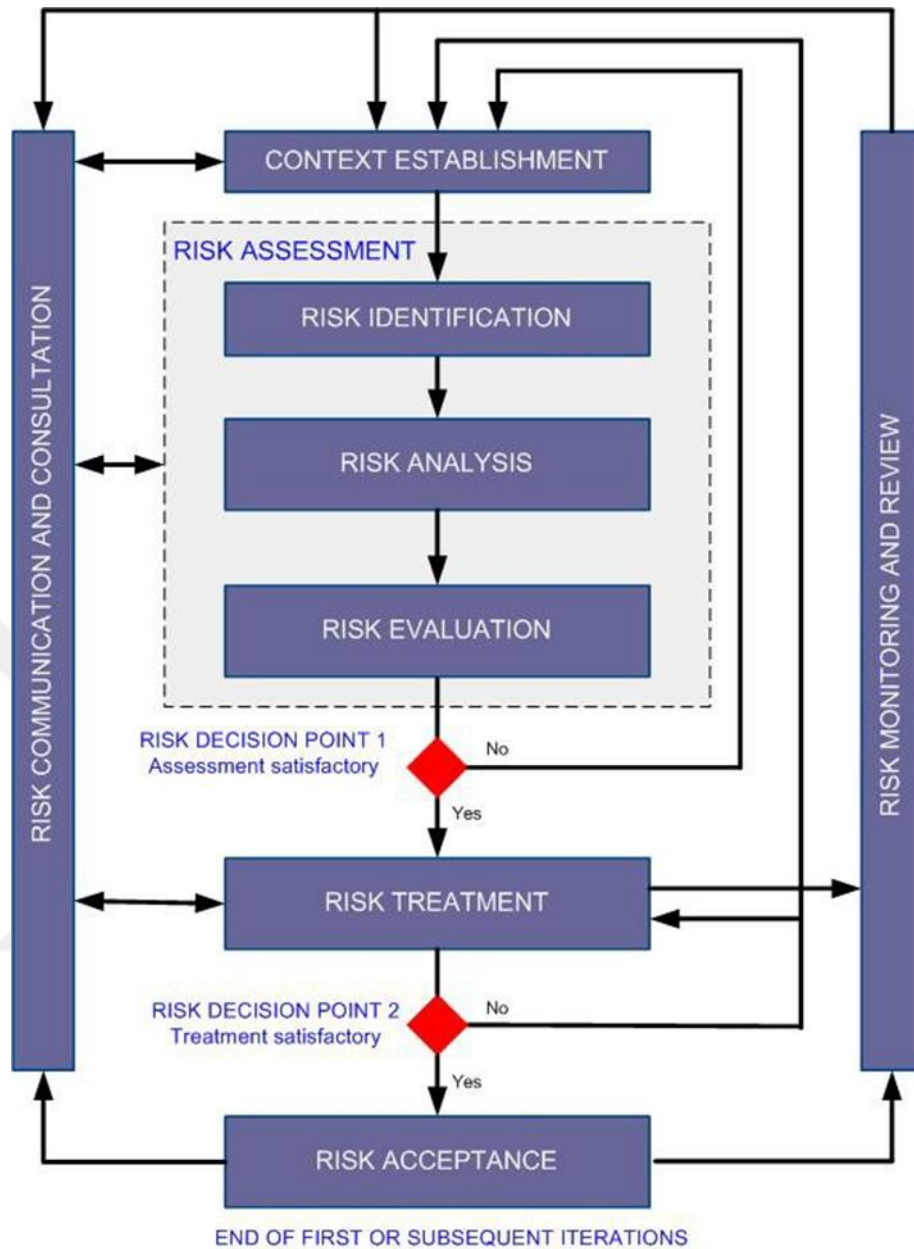
#### **4.6 ISO/IEC 27005**

ISO/IEC 27005:2011 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach [25]. The official full name of this standard is “ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management”.

It refers ISO/IEC 27000 and the 2005 version of ISO/IEC 27001 as normative and basic standards, and mentions ISO/IEC 27002 in the scope section.

The standard doesn't offer a specific risk management method. It does however define a continual process with a structured sequence of activities, some of which are iterative. The content of the standard is related with security risk management process, which illustrated in Figure 4.3 [25].

The information security risk management process consists of context establishment (Clause 7), risk assessment (Clause 8), risk treatment (Clause 9), risk acceptance (Clause 10), risk communication and consultation (Clause 11), and risk monitoring and review (Clause 12) [25].



**Figure 4.3** Information security risk management processes

## 4.7 ISO/IEC 27006

ISO/IEC 27006:2015 specify requirements and provide guidance for bodies providing audit and certification of an ISMS, in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification [26]. The official full name of this standard is “ISO/IEC 27006:2015 Information

technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems”.

The purpose of ISO/IEC 27006 is to “supplements ISO/IEC 17021 in providing the requirements by which certification organizations are accredited, thus permitting these organizations to provide compliance certifications consistently against the requirements set forth in ISO/IEC 27001” [2].

The chapters within the standard are as follows: Scope, References, Terms, Principles, General Requirements, Structural Requirements, Resource Requirements, Information Requirements, Process Requirements, Management System Requirements.



# CHAPTER 5

## DEVELOPMENT TOOLS AND ENVIRONMENTS

The ISMS Search Tool is designed as a web-based application, since it provides many advantages over desktop applications. It is also intended to develop a flexible tool. In this context, web based application provide many advantages.

On the other hand, open source platforms and tools are also preferred while developing this search tool due to they have many benefits. Some of the open source platforms and tools that used while developing phase are; PHP, MySQL, Apache Server, XAMPP, Notepad++, StarUML, MySQL Work Bench.

PHP is used as the server side programming language and also MySQL selected as a database management system. Detail information about platforms that used while developing tool will be given below.

### **5.1 Concepts and Advantages of Open Source**

Open source software is usually developed by a group or community, free to use and redistribution. It is also offered free access to source codes thus everyone can view, edit or change hence everyone contribute to the project. Open source also provides many advantages. Some of them will be outlined briefly in this title.

The use of open source software is generally free or cheaper to use and it is available to modify and distribute. It has lower costs and typically when used for commercial the cost is also low.

It is accepted that open-source software is more secure than proprietary ones because source code is accessible and anyone able to improve software, fix bugs, and maintain to develop it. Thus, users do not need to wait for updates. Users can also be sure that there aren't any suspicious particles in source codes. On the other hand, it shouldn't be forgotten the source code, which can be seen by everyone may be a threat at the same time. For this reason, the open source software must keep in up to date.

## 5.2 Web Based Applications

A Web-based application refers to any software that is accessed over a network connection using HTTP (Hyper-Text Transfer Protocol), rather than existing within a local computer. Web-based applications often run on web browser. However, Web-based applications also may be client-based, where a part of the program is downloaded to a user's computer or mobile device, but processing is done over the Internet on an external server. Some of the benefits of using web-based application are briefly listed below.

No need installation on each computer or mobile device. Web based applications are easy to access through any web browser like Internet Explorer, Google Chrome, Mozilla Firefox etc. so users access the applications via a uniform environment.

No need to redesign software for each operating systems or platforms. Web-based applications need only be developed for a single platform and can be used in all platforms. This makes development and troubleshooting much easier.

Differently from traditional applications, web based applications can be accessible anytime, anywhere by using any device like computer, smartphone, tablet, pc etc. Users just only need an internet connection.

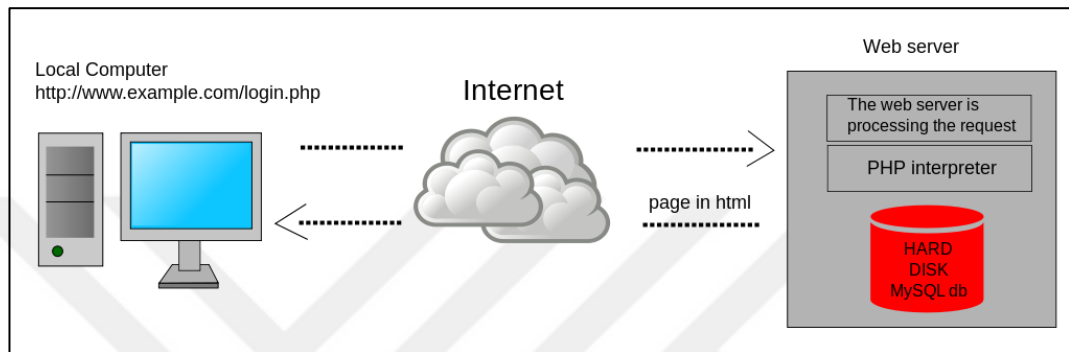
The user interface of web-based applications is easier to customize than it is in desktop applications. This makes it easier to update the look and feel of the application, or to customize the presentation of information to different user profiles.

Installation and maintenance becomes less complicated. Web-based applications are typically deployed only server side, which are monitored and maintained by professional server administrators. This is far more effective than monitoring many of client computers.

As a result, web-based software provides benefits during both the development, installation and maintenance.

## 5.3 PHP

PHP (recursive acronym for PHP: Hypertext Preprocessor) is a widely-used open source general-purpose scripting language that is especially suited for web development and can be embedded into HTML [27].



**Figure 5.1** Server side programming schema

PHP is a server site programming language that can process data sent from browser and produce content on the server side, and sends produced content to the client browser as seen in Figure 5.1.

### What is PHP

- PHP known as Hypertext Preprocessor is a recursive acronym
- PHP is a server side scripting which is embedded with HTML
- PHP used to manage Content Management System, dynamic content, databases, ecommerce sites, and application tool
- PHP is an open source scripting language. It is free to use and download
- PHP support most of all databases like as MySQL, PostgreSQL, Sybase, Oracle, MicrosoftSQL
- POP3, IMAP, LDAP and a large number of major protocols support PHP

## 5.4 MySQL

MySQL is the most popular Open Source SQL database management system. It is developed, distributed, and supported by Oracle Corporation under GNU General Public License.

MySQL is also a relational database management system (RDBMS). A relational database stores data in separate tables rather than putting all the data in one big storeroom. The database structures are organized into physical files optimized for speed. The logical model, with objects such as databases, tables, views, rows, and columns, offers a flexible programming environment. You set up rules governing the relationships between different data fields, such as one-to-one, one-to-many, unique, required or optional, and “pointers” between different tables. The database enforces these rules, so that with a well-designed database, your application never sees inconsistent, duplicate, orphan, out-of-date, or missing data [28].

## 5.5 Apache HTTP Server

Apache is the most widely used open source web server software [29]. Developed and maintained by Apache Software Foundation and it is available for free.

A web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients. Dedicated computers and appliances may be referred to as web servers as well [30].

A web server's job is basically to accept requests from clients and send responses to those requests. A web server gets a URL, translates it to a filename (for static requests), and sends that file back over the internet from the local disk, or it translates it to a program name (for dynamic requests), executes it, and then sends the output of that program back over the internet to the requesting party. If for any reason, the web server was not able to process and complete the request, it instead returns an error message. The word, web server, can refer to the machine (computer/hardware) itself, or the software that receives requests and sends out responses [31].

## **5.6 XAMPP**

There are some difficulties of installing MySQL and PHP server to the computer separately so developers prefer an installer package which include all in one executable file. The XAMPP solves this problem. The XAMPP word is formed from the initials of the words of Cross-Platform (X), Apache (A), MySQL (M), PHP (P) and Perl (P).

XAMPP is a simple Apache Friends Community distribution that makes it extremely easy for developers to create a local web server for testing purposes. Everything you need to set up a web server – server application (Apache), database (MySQL), and scripting language (PHP) – is included in a simple extractable file.

Official web address is “<https://www.apachefriends.org>”.

## **5.7 Notepad++**

Software developers need an editor to reduce spending time for writing code. Notepad++ is a source code editor that supports several languages and distributed under GPL License.

Official web address is “<https://notepad-plus-plus.org/>”.

## **5.8 StarUML**

StarUML is a software modeling platform that supports UML (Unified Modeling Language). It actively supports the MDA (Model Driven Architecture) approach by supporting the UML profile concept. StarUML excels in customizability to the user’s environment and has a high extensibility in its functionality.

## **5.9 MySQL Workbench**

MySQL Workbench is a unified visual tool for database architects, developers, and DBAs. MySQL Workbench provides data modeling, SQL development, and comprehensive administration tools for server configuration, user administration,



backup, and much more. MySQL Workbench enables a DBA, developer, or data architect to visually design, model, generate, and manage databases.



# CHAPTER 6

## IMPLEMENTATION

### 6.1 Introduction

ISMS Search Tool is designed to help people who are interested in information security and work with information security standards. It is intended to make working with information security management standards much easier and efficient. When designing this tool, it was aimed to be simple, understandable, and efficient.

Implementation of the tool will be explained throughout this chapter. The structure of the chapter is as follows;

- Application architecture; defining a structured solution that meets all of the technical and operational requirements
- Database design; describing in detail the data model of the database
- Software design; explaining the process of defining software methods, functions, objects, and the overall structure and interaction
- Administration Panel; in this section the administration panel and its functionality are presented step by step
- End-User Panel; in this part the main interface of the tool is explained

### 6.2 Software Architecture

This section provides an architectural overview of the tool. It is intended to capture and convey the significant architectural decisions, which have been made on the tool. The overall scenario of the tool is illustrated in Figure 6.1 and a layered software architecture design schema is given in Figure 6.2.

Use Case View is an important input to the selection of the set of scenarios and use cases that are the focus of iteration. It describes the set of scenarios and use cases that

represent the significant and central functionality. These use cases are described related topics in section 6.5 and 6.6.

The Search Tool Administration Panel use cases are:

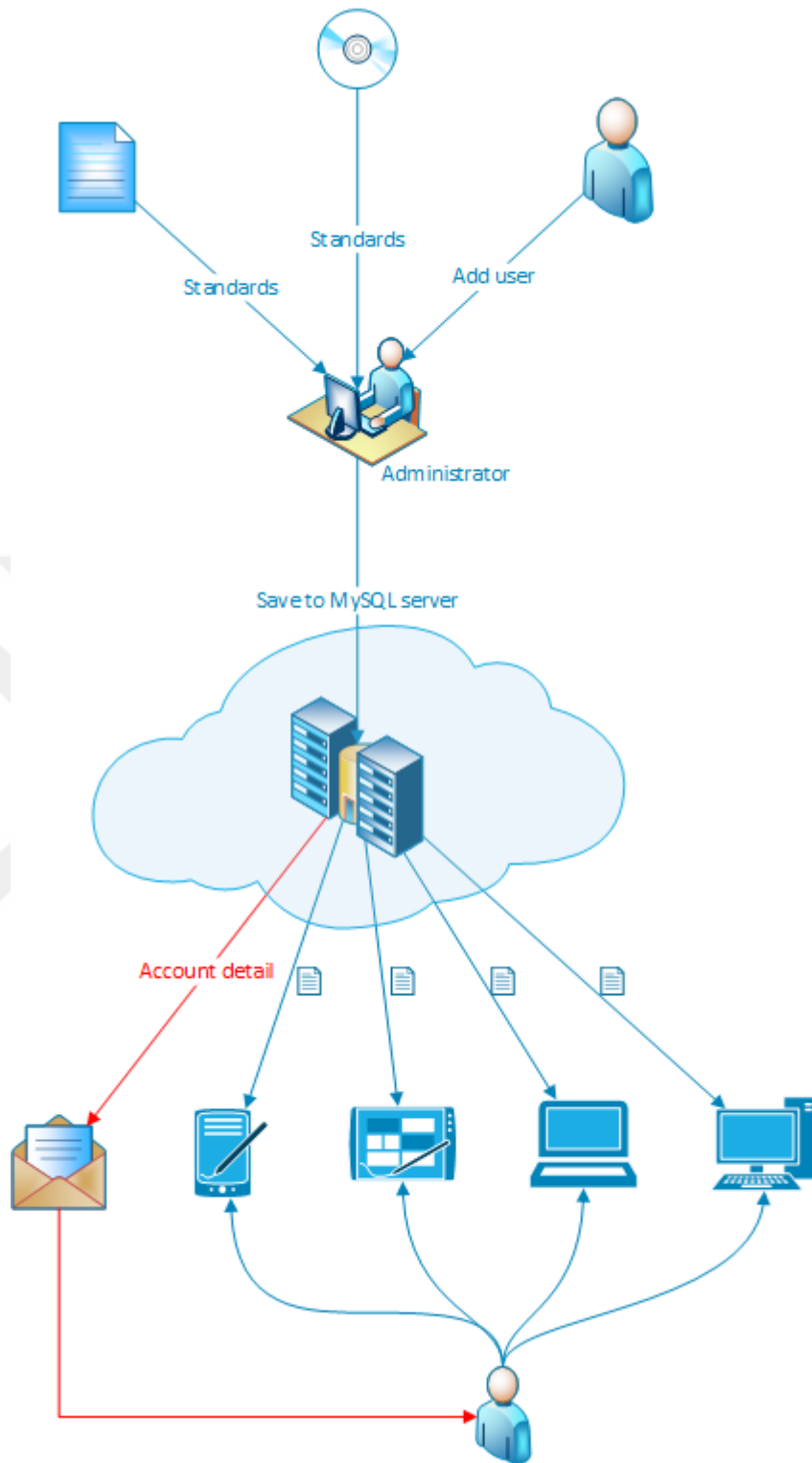
- Login to admin panel (Authentication control)
- Manage standards as a source
- Manage content of the standard
- Manage users
- Logout admin panel

The administrator initiates these use cases.

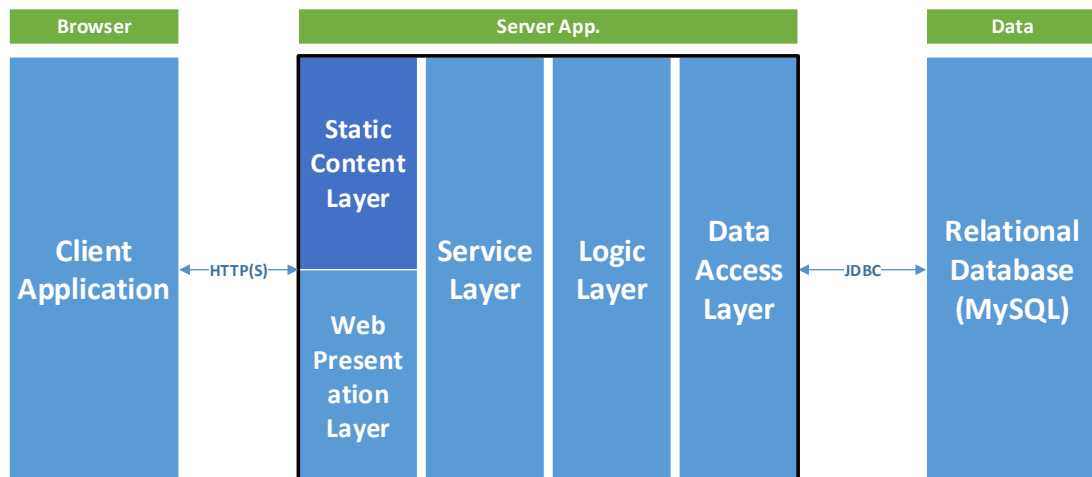
The Search Tool End User use cases are:

- Search keyword on selected standard(s)
- Analyze frequency of keyword
- Compare standards

These use cases are initiated by the normal-user.



**Figure 6.1** The search tool application scenario



**Figure 6.2** Layered software architecture

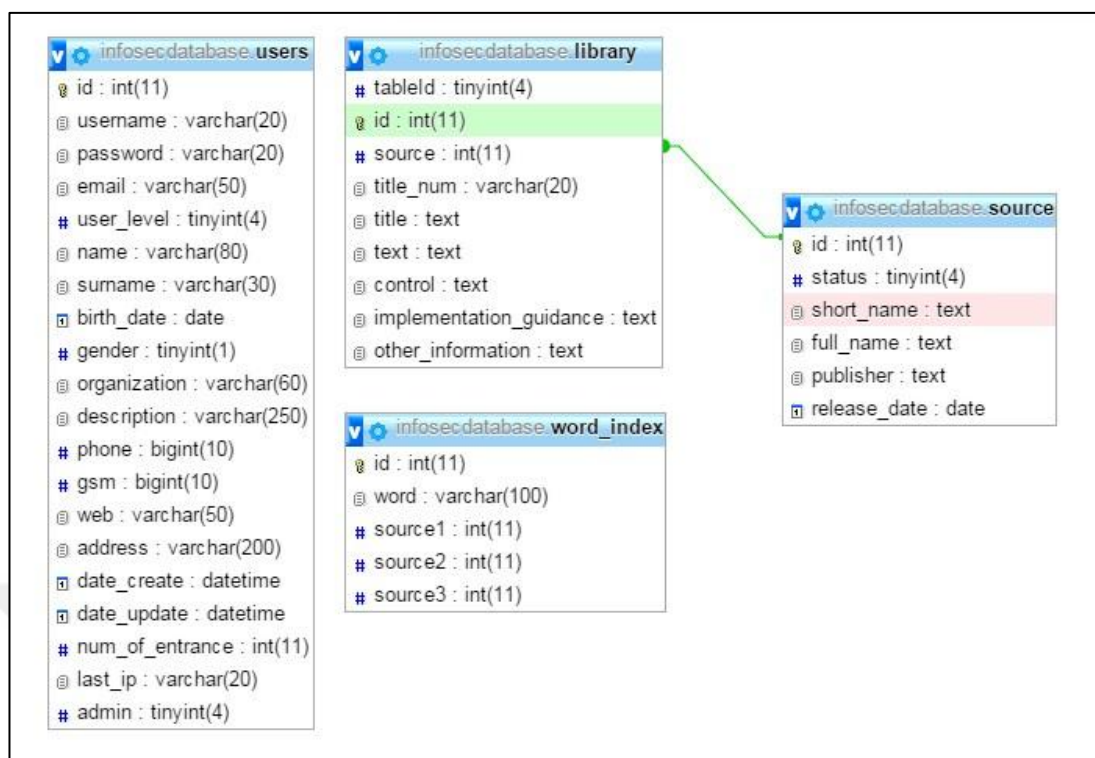
### 6.3 Database Design

The key to a successful application is its database design and this is why a lot of thought and effort was put into this phase. In the design phase, the relational database model is preferred which adds many advantages.

The relational model (RM) for database management is an approach to managing data using a structure and language consistent with first-order predicate logic and first described in 1969 by Edgar F. Codd [32].

In the relational model, all data must be stored in tables, and these tables connected with each other by using a unique value called as primary key value. Tables have columns that store unique values to identify the row. In another interconnected table have also a column that contain values too, which is the same value that a referenced table has. Thus tables can be connected with each other by using the same value named as primary key value, this database method named as relational database.

The relational database design of the tool is shown in Figure 6.3 and an entity-relationship (ER) model is also given in Figure 6.4. ER Model is a method that represent a logical relationship of objects (or entities) graphically in order to create database.



**Figure 6.3** Database design for the ISMS search tool

The Database of the tool consists of four tables. One of them is ‘users’ table which is not related to any table and is used to store user information that makes only authorized users manage and work on standards.

The other three tables are related to the subject of this study directly. These are: ‘source’, ‘library’ and ‘word\_index’ tables. Information about standards which are loaded to the database be used by the tool is stored in the ‘source’ table. The source table stores only main information about standards like name, published date, author etc. The ‘library’ table stores the data content of the standards.

Finally, ‘word\_index’ table contains words and number of repetition of the words in the standards. Relationship of the tables can be seen in Figure 6.3. As seen in the E-R diagrams of the tool, the library table is joined to the source table by source id value.

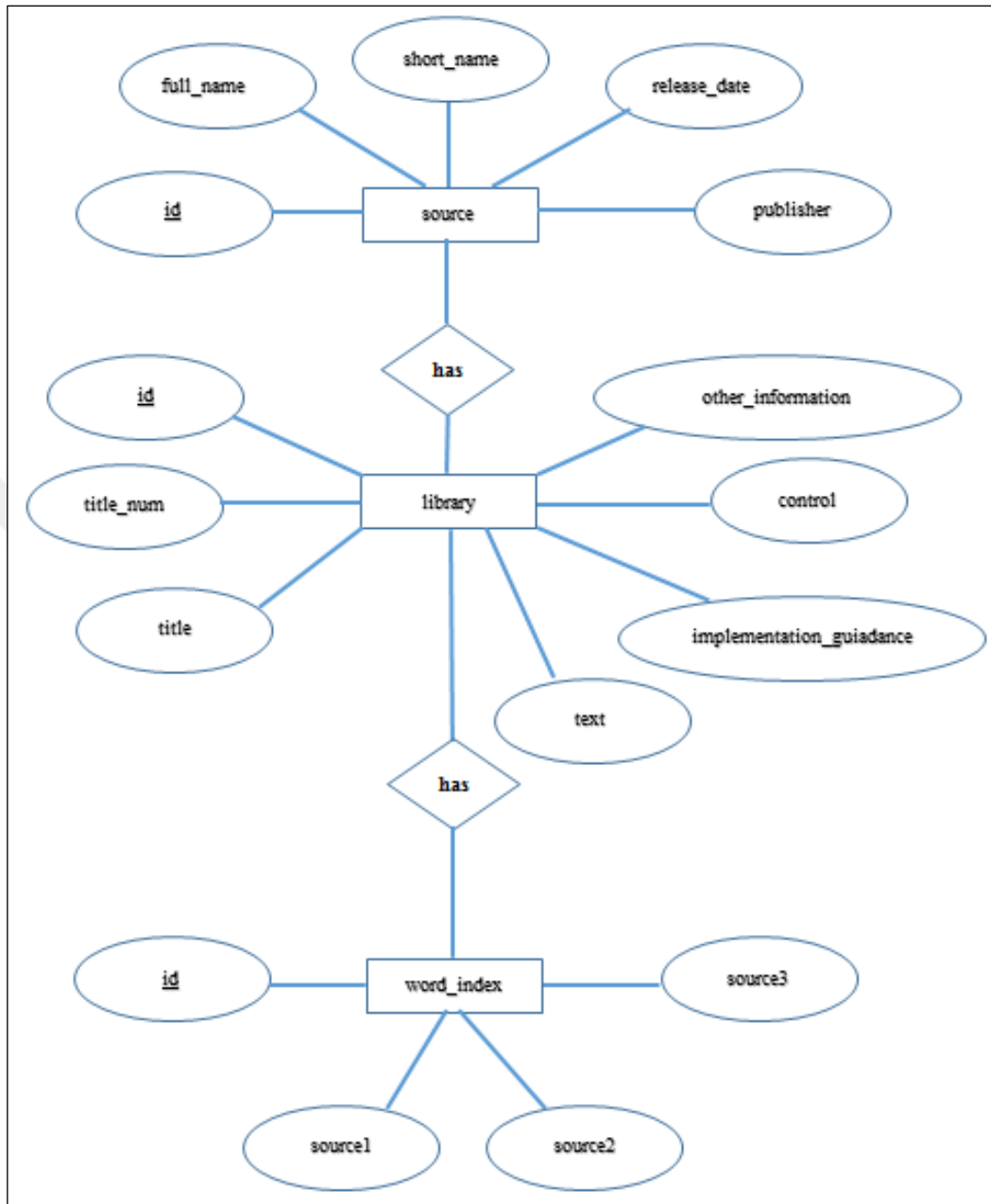


Figure 6.4 E-R diagram for the ISMS search tool

## **6.4 Software Design**

In this section software design of the search tool is explained. Normally, this section can be expected to be a separate chapter in itself. However, to maintain the simplicity of the thesis the 'Software Design' arranged as a subheading under the 'Implementation' title. If it had been given as a separate chapter, the following titles 'Administration Panel' and 'End-User Panel' could be a subheading for this chapter.

In design and development phase, open source platforms and tools are preferred because of its considerable advantages which is mentioned before in section 5.1. Therefore, PHP as a scripting language and MySQL as a database engine are chosen.

PHP is suited for web development and can be embedded into HTML. PHP can work with virtually all database software, including Oracle and Sybase but most commonly used is the freely available MySQL database.

This search tool consists of two modules. First one is administrator module and second one is end-user module. In administration module, administrative user is able to load ISMS standards to database and can manage all standards in one interface. In addition, the administrator can also add new users to database to make user available to reach and work on ISMS standards.

On the other hand, end-user module provides authorized users to search for keywords in standards, analyze them, and compare all standards between each other.

## **6.5 Administration Panel**

In the administration module administrator can manage other users and standards. First, user management is for authorization to let users reach and work with standards. Due to copyright of documents only users with license can be added and authorized.

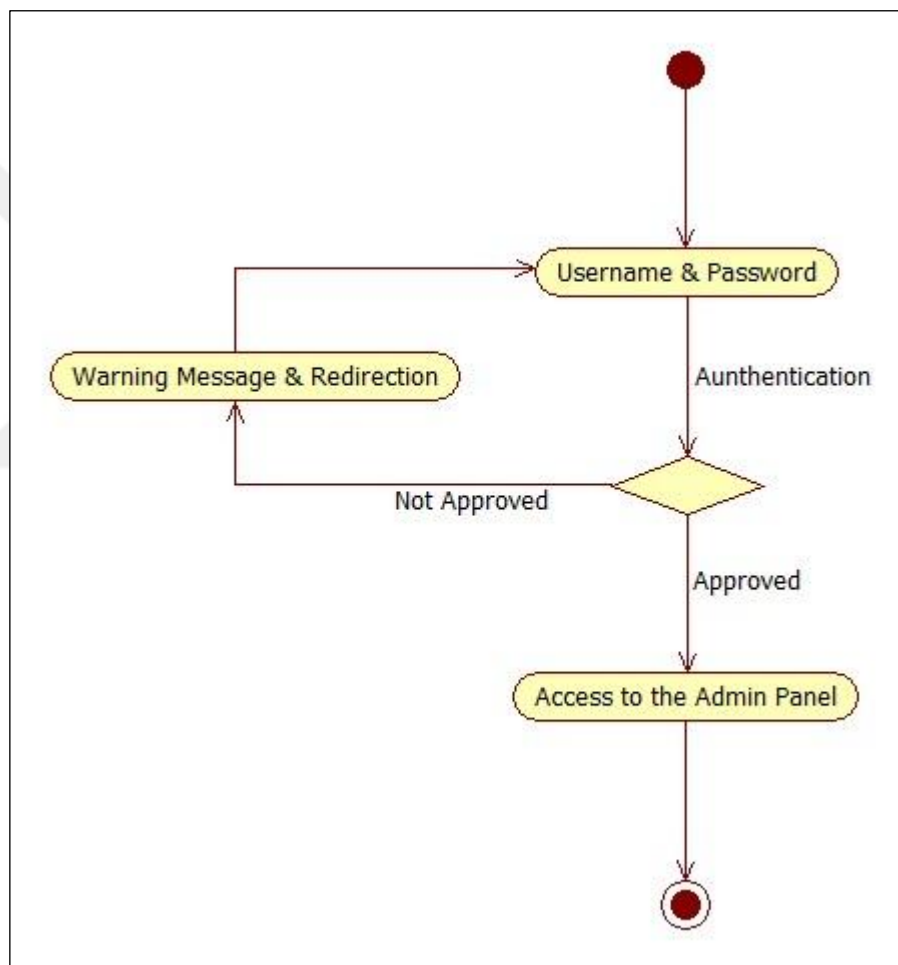
Second is source management. In source management, standards as a source can be loaded to database, modified and can be deleted. Another feature of the admin module is a word counter which counts all words in each document stored in the



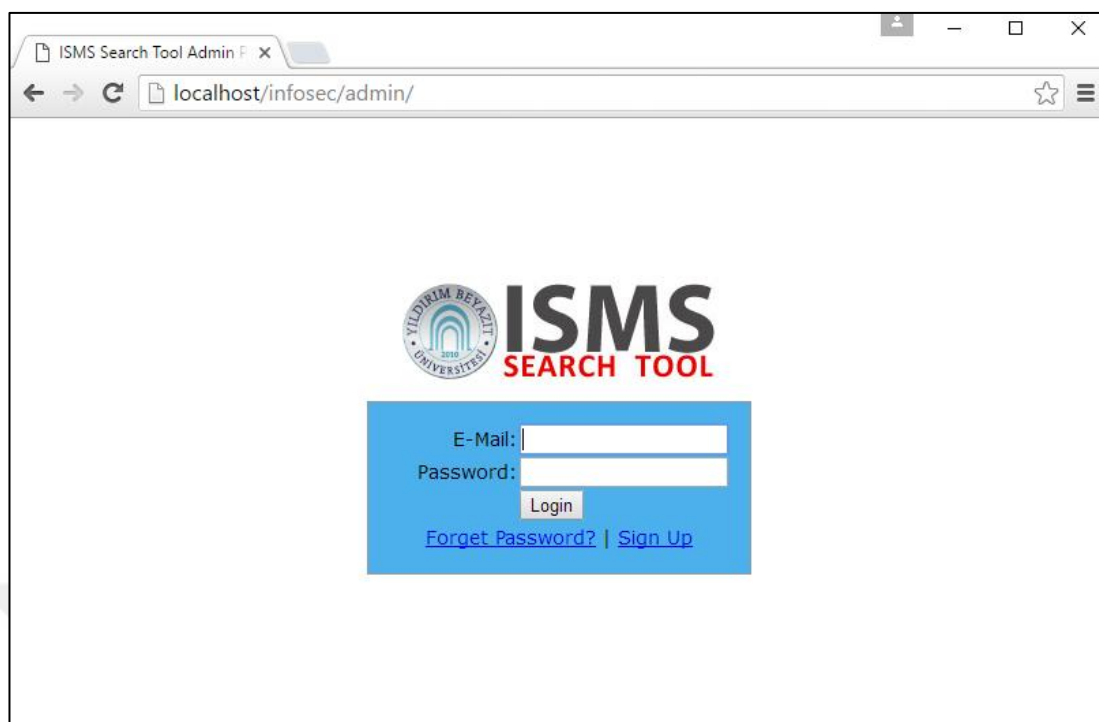
database. This script creates a list of words passed in standards, and calculates how many times a word is repeated in a standard.

### 6.5.1 Authentication Control

There is an authentication control to reach admin module which activity diagram shown in Figure 6.5. Users that have administrative authority uses a mail address and a password to log in to the administration panel. The screenshot of the login page is shown in Figure 6.6.



**Figure 6.5** Activity diagram for authentication



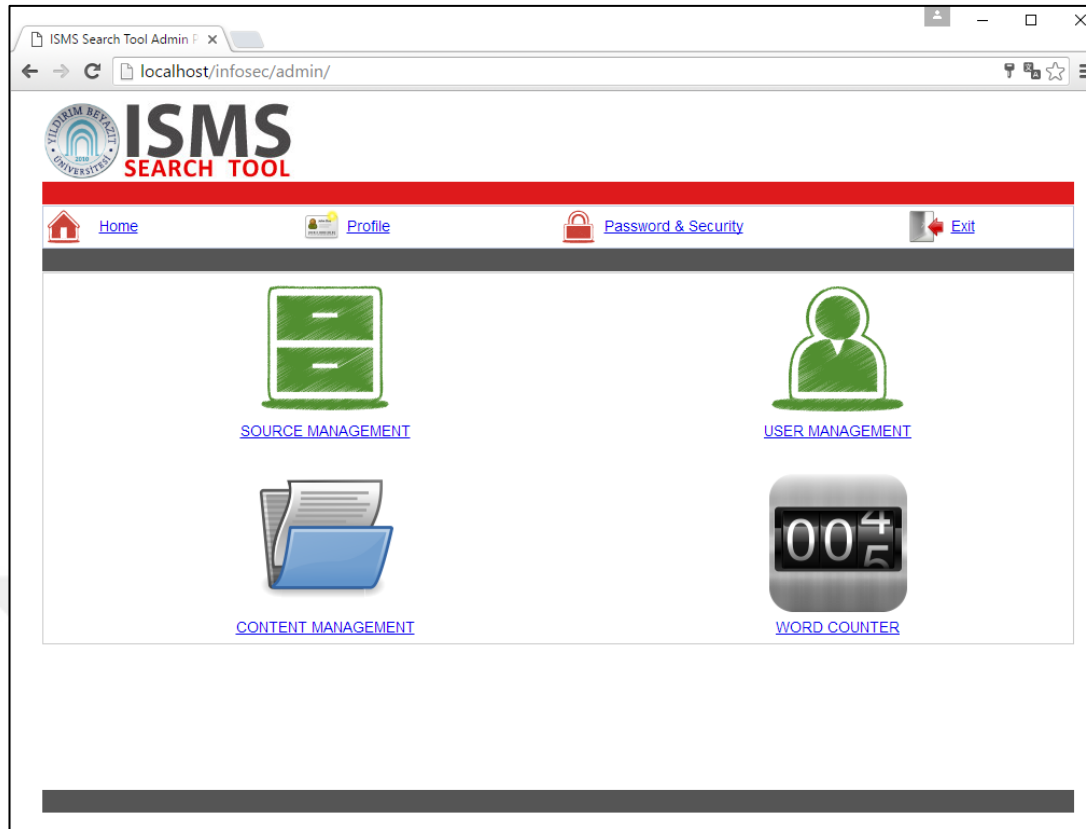
**Figure 6.6** Administration panel login page

### **6.5.2 Administration Panel Main Page**

The main page of the administration panel is shown in Figure 6.7. The intention of the design phase was for the tool to be easy to use for the end users of all levels.

There are four buttons as links on the main page of the administration panel. These are used to access the following sections of the module; Source Management, Content Management, User Management and Word Counter. Detailed information about these sections will be given in each related topic.

The links on the upper side of the administration panel is concerned with the operation of the logged user. The end user can change his/her password and other personal information by using these links on the admin panel.



**Figure 6.7** Administration panel main page

### **6.5.3 Source Management**

In this tool, ISMS standards are named as source. Standards need to be loaded to the database as source in order to work on them. Before loading standards to the database, a profile for standard which includes basic information about standard such as official name, publisher, published date etc. must be created. In source management, administrator can create this profile for the standards.

In the source management, the administrator can also delete, re-cover, edit, block, unblock and destroy operations. These operations will be explained respectively below and a screen shot of main page of the source management is given in Figure 6.8.

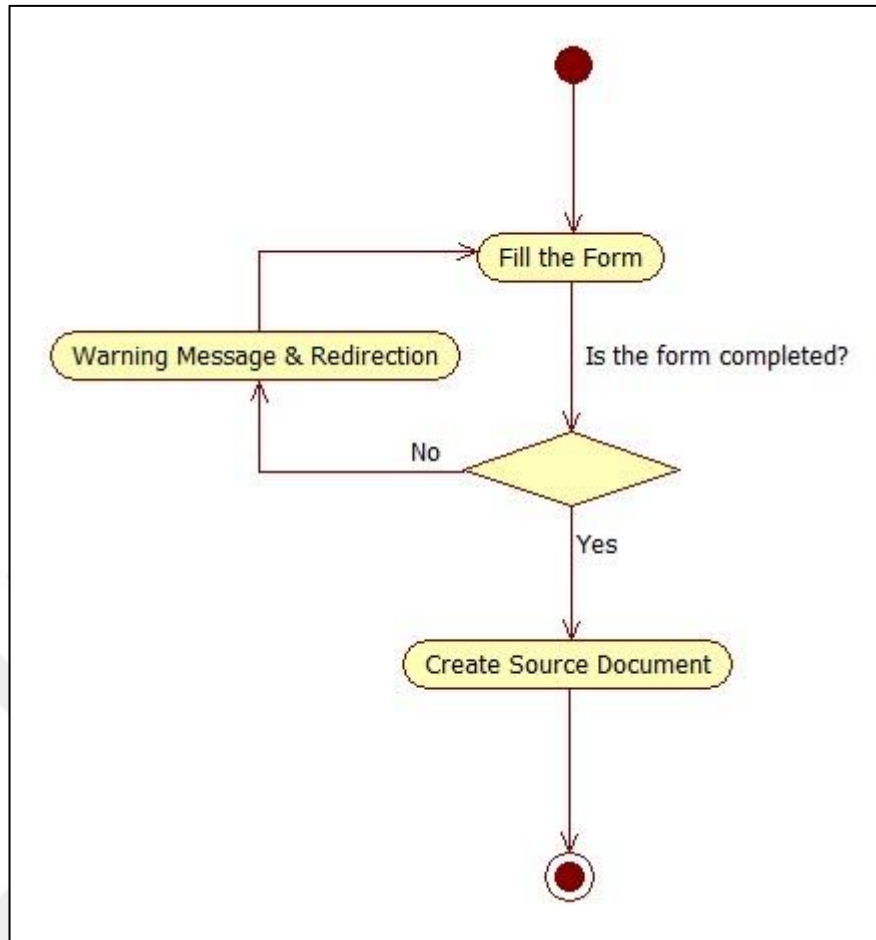
Source ID	Status	Short Name	Full Name	Publisher	Release Date	Operations
1	✓	ISO/IEC 27000:2014	Information technology — Security techniques — Information security management systems — Overview and vocabulary	ISO/IEC JTC 1/SC 27	2014-01-15	
2	✓	ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements	ISO/IEC JTC 1/SC 27	2013-10-01	
3	✓	ISO/IEC 27002:2013	Information technology — Security techniques — Code of practice for information security controls	ISO/IEC JTC 1/SC 27	2013-10-01	
4	✓	ISO/IEC 27003:2010	Information technology — Security techniques — Information security management system implementation guidance	ISO/IEC JTC 1/SC 27	2010-02-01	
5	✓	ISO/IEC 27004:2009	Information technology — Security techniques — Information security management — Measurement	ISO/IEC JTC 1/SC 27	2009-12-15	
6	✓	ISO/IEC 27005:2011	Information technology — Security techniques — Information security risk management	ISO/IEC JTC 1/SC 27	2011-06-01	
7	✓	ISO/IEC 27006:2015	Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems	ISO/IEC JTC 1/SC 27	2015-10-01	
8	✗	ISO/IEC 27007:2011	Information technology — Security techniques — Guidelines for information security management systems auditing	ISO/IEC JTC 1/SC 27	2011-11-15	

**Figure 6.8** Source management main page

### 6.5.3.1 Creating New Source Profile

It is possible to add new standards to the database to increase extensibility and scalability of the tool. Before uploading documents of standard to the database, it is necessary to create a profile of a standard. After creating profile, contents of standard adding to the database manually.

An activity diagram of the process shown in the following Figure 6.9.




**Figure 6.9** Activity diagram for creating a new source

To create a new source profile, the link named as ‘Create New Source’ which is stated under the ‘Source Management’ is used. The profile is created by filling out the form completely on the screen in Figure 6.11 which can be initiated by the link seen in Figure 6.10.

The screenshot displays the ISMS Search Tool interface. At the top, there is a navigation bar with links for Home, Profile, Password & Security, and Exit. Below this, the page title is 'Source Management > Source List'. The main content is a table with the following columns: Source ID, Status, Short Name, Full Name, Publisher, Release Date, and Operations. The table lists nine entries, each with a status icon (green checkmark or red X) and a set of operation icons (edit, delete, refresh, etc.). A red arrow points to a 'Create New Source' button located at the bottom left of the interface.

Source ID	Status	Short Name	Full Name	Publisher	Release Date	Operations
1	✓	<a href="#">ISO/IEC 27000:2014</a>	<a href="#">Information technology — Security techniques — Information security management systems — Overview and vocabulary</a>	ISO/IEC JTC 1/SC 27	2014-01-15	[Icons]
2	✓	<a href="#">ISO/IEC 27001:2013</a>	<a href="#">Information technology — Security techniques — Information security management systems — Requirements</a>	ISO/IEC JTC 1/SC 27	2013-10-01	[Icons]
3	✓	<a href="#">ISO/IEC 27002:2013</a>	<a href="#">Information technology — Security techniques — Code of practice for information security controls</a>	ISO/IEC JTC 1/SC 27	2013-10-01	[Icons]
4	✓	<a href="#">ISO/IEC 27003:2010</a>	<a href="#">Information technology — Security techniques — Information security management system implementation guidance</a>	ISO/IEC JTC 1/SC 27	2010-02-01	[Icons]
5	✓	<a href="#">ISO/IEC 27004:2009</a>	<a href="#">Information technology — Security techniques — Information security management — Measurement</a>	ISO/IEC JTC 1/SC 27	2009-12-15	[Icons]
6	✓	<a href="#">ISO/IEC 27005:2011</a>	<a href="#">Information technology — Security techniques — Information security risk management</a>	ISO/IEC JTC 1/SC 27	2011-06-01	[Icons]
7	✓	<a href="#">ISO/IEC 27006:2015</a>	<a href="#">Requirements for bodies providing audit and certification of information security management systems</a>	ISO/IEC JTC 1/SC 27	2015-10-01	[Icons]
8	✗	<a href="#">ISO/IEC 27007:2011</a>	<a href="#">Information technology — Security techniques — Guidelines for information security management systems auditing</a>	ISO/IEC JTC 1/SC 27	2011-11-15	[Icons]
9	✗	<a href="#">ISO/IEC TR 27008:2011</a>	<a href="#">Information technology — Security techniques — Guidelines for auditors on information security controls</a>	ISO/IEC JTC 1/SC 27	2011-10-15	[Icons]

 [Create New Source](#)

**Figure 6.10** Create new source button

Before loading a new source, a profile that contains the basic information must be created. The link seen in Figure 6.10 must be clicked to invoke the ‘Create a New Source’ form.

The screenshot shows a web browser window with the URL `localhost/infosec/admin/?p=managesource&is=newsource`. The page header includes the Yildirim Beyazit University logo and the text "ISMS SEARCH TOOL". A navigation bar contains links for "Home", "Profile", "Password & Security", and "Exit". Below the navigation bar, the breadcrumb "Source Management > Create New Source >" is visible. The main content area is titled "Create New Source" and contains a form with the following fields:

Short Name*	<input type="text" value="ISO/IEC 27007"/>
Full Name*	<input type="text" value="Information technology --"/>
Publisher*	<input type="text" value="ISO/IEC JTC 1/SC 27"/>
Release Date* (YYYY-MM-DD)	<input type="text" value="2011-11-15"/>

At the bottom of the form is a "Submit" button.

**Figure 6.11** Form for adding a new source

The form was kept quite short to ensure simplicity and user-friendliness and in order to complete the process all fields must be filled in as it appears in Figure 6.11.

The screenshot shows the ISMS Search Tool interface. At the top, there is a navigation bar with links for Home, Profile, Password & Security, and Exit. Below this, the breadcrumb 'Source Management > Source List' is visible. A yellow notification box displays the message: 'Congrats! The source has been created successfully.' Below the notification is a table listing various ISO/IEC standards. A red arrow points to the bottom row of the table, which is highlighted in yellow. This row represents the newly added source.

Source ID	Status	Short Name	Full Name	Publisher	Release Date	Operations
1	✓	<a href="#">ISO/IEC 27000:2014</a>	<a href="#">Information technology — Security techniques — Information security management systems — Overview and vocabulary</a>	ISO/IEC JTC 1/SC 27	2014-01-15	
2	✓	<a href="#">ISO/IEC 27001:2013</a>	<a href="#">Information technology — Security techniques — Information security management systems — Requirements</a>	ISO/IEC JTC 1/SC 27	2013-10-01	
3	✓	<a href="#">ISO/IEC 27002:2013</a>	<a href="#">Information technology — Security techniques — Code of practice for information security controls</a>	ISO/IEC JTC 1/SC 27	2013-10-01	
4	✓	<a href="#">ISO/IEC 27003:2010</a>	<a href="#">Information technology — Security techniques — Information security management system implementation guidance</a>	ISO/IEC JTC 1/SC 27	2010-02-01	
5	✓	<a href="#">ISO/IEC 27004:2009</a>	<a href="#">Information technology — Security techniques — Information security management — Measurement</a>	ISO/IEC JTC 1/SC 27	2009-12-15	
6	✓	<a href="#">ISO/IEC 27005:2011</a>	<a href="#">Information technology — Security techniques — Information security risk management</a>	ISO/IEC JTC 1/SC 27	2011-06-01	
7	✓	<a href="#">ISO/IEC 27006:2015</a>	<a href="#">Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems</a>	ISO/IEC JTC 1/SC 27	2015-10-01	
9	✗	<a href="#">ISO/IEC TR 27008:2011</a>	<a href="#">Information technology — Security techniques — Guidelines for auditors on information security controls</a>	ISO/IEC JTC 1/SC 27	2011-10-15	
10	✓	<a href="#">ISO/IEC 27007</a>	<a href="#">Information technology -- Security techniques -- Guidelines for information security management systems auditing</a>	ISO/IEC JTC 1/SC 27	2011-11-15	

**Figure 6.12** A notification after adding a new source

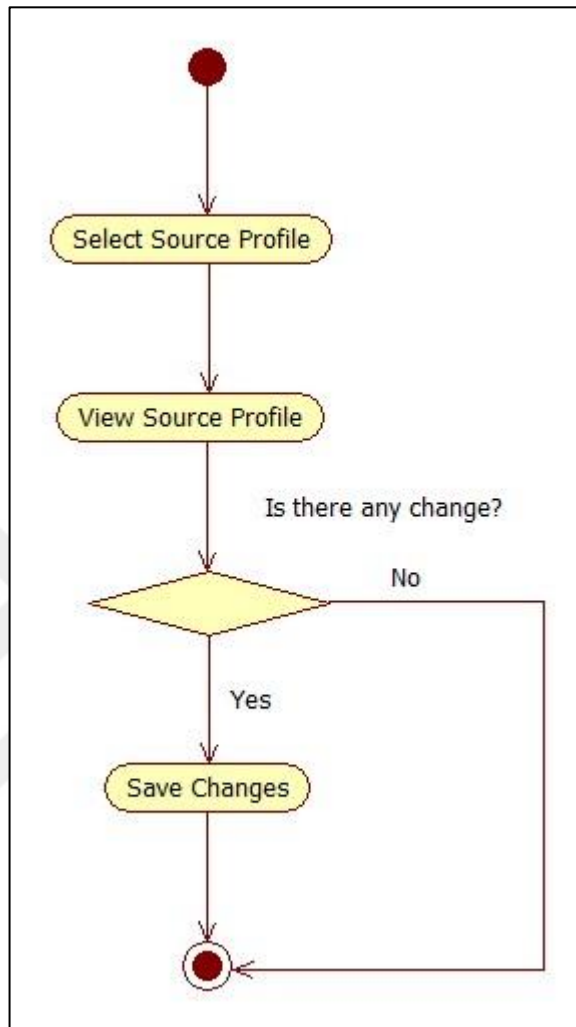
Unless there is an error, when the form is filled in and the confirmation button is pressed, the process will be completed successfully. A notification message will be displayed indicating that the operation was successful shown in Figure 6.12. In addition, the newly created profile can be seen on the same screen at the bottom line of the source list.

### 6.5.3.2 View/Edit Source Profile

End users are able to view or change the attributes of the source profile after creating it. Edit icon at the bottom of the source list is used to initiate the edit process.









After clicking the icon, the process given in the activity diagram in Figure 6.13 begins.



**Figure 6.13** Activity diagram for view/edit source processes

As seen from the activity diagram in Figure 6.13, user first selects a source by clicking the edit icon seen in Figure 6.14 so it displays source information.

Source ID	Status	Short Name	Full Name	Publisher	Release Date	Operations
1	✓	ISO/IEC 27000:2014	Information technology — Security techniques — Information security management systems — Overview and vocabulary	ISO/IEC JTC 1/SC 27	2014-01-15	  
2	✓	ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements	ISO/IEC JTC 1/SC 27	2013-10-01	  

**Figure 6.14** Editing a source

After clicking the edit icon, a form is displayed as shown in Figure 6.15.

ISMS Search Tool Admin

localhost/infosec/admin/?p=managesource&is=edit&id=1

**View/Edit Source**

Short Name\*

Full Name\*




Publisher\*

Release Date\* (YYYY-MM-DD)

**Figure 6.15** Form for view/edit a source

After editing the source information and submitting the form, the tool checks the changes. If a change is detected by the software, it is saved to the database and a notification message is displayed seen in Figure 6.16.

The screenshot shows the ISMS Search Tool interface. At the top, there is a navigation bar with links for Home, Profile, Password & Security, and Exit. Below this, the page title is "Source Management > Source List". A yellow notification box displays the message: "Congrats! The source has been updated successfully." Below the notification is a table with the following columns: Source ID, Status, Short Name, Full Name, Publisher, Release Date, and Operations. The first row of the table contains the following data: Source ID: 1, Status: a green checkmark icon, Short Name: ISO/IEC 27000:2016, Full Name: Information technology — Security techniques — Information security management systems — Overview and vocabulary, Publisher: ISO/IEC JTC 1/SC 27, Release Date: 2016-02-15, and Operations: three icons (a pencil, a trash can, and a red stop sign). Red arrows point from the notification box to the Short Name and Release Date cells in the table.

Source ID	Status	Short Name	Full Name	Publisher	Release Date	Operations
1	✓	ISO/IEC 27000:2016	Information technology — Security techniques — Information security management systems — Overview and vocabulary	ISO/IEC JTC 1/SC 27	2016-02-15	  

**Figure 6.16** A notification after editing a source

### 6.5.3.3 Block and Unblock Source Profile

Standards which are used as a source in the search tool can be blocked or unblocked to be reached by users. Small activate and block icon on the right side of the source list is used to block or activate a source to access. By default, the source document is created as open access. It is noticed with the green color “active” icon in the status column shown in Figure 6.18 in the source list. Source document can be closed to access by clicking the block icon in operation column. When source is blocked to access, an activation icon occurs in operation column and blocked icon appear in status column (Figure 6.17).

The screenshot shows the ISMS Search Tool interface. At the top, there is a navigation bar with links for Home, Profile, Password & Security, and Exit. Below this, the breadcrumb 'Source Management > Source List' is visible. A yellow notification banner states 'The source has been blocked!'. Below the notification is a table with the following data:

Source ID	Status	Short Name	Full Name	Publisher	Release Date	Operations
1		<a href="#">ISO/IEC 27000:2016</a>	<a href="#">Information technology — Security techniques — Information security management systems — Overview and vocabulary</a>	ISO/IEC JTC 1/SC 27	2016-02-15	
2		<a href="#">ISO/IEC 27001:2013</a>	<a href="#">Information technology — Security techniques — Information security management systems — Requirements</a>	ISO/IEC JTC 1/SC 27	2013-10-01	

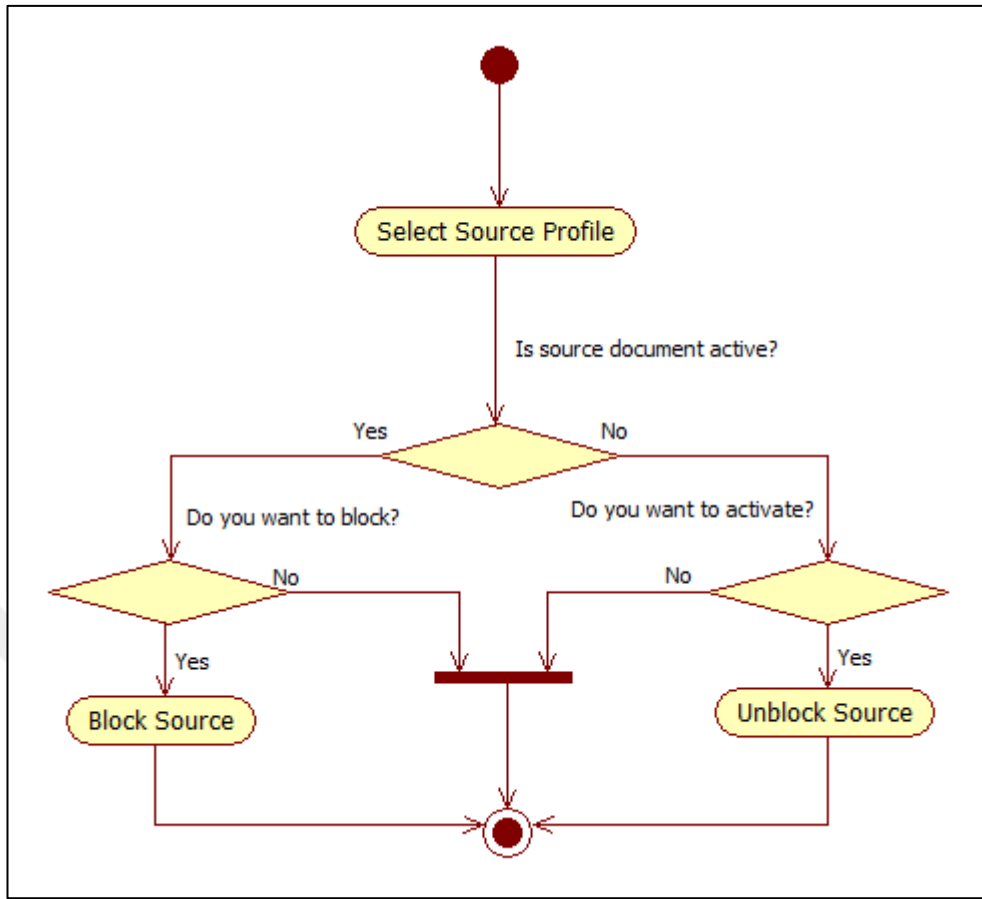
Figure 6.17 Block / unblock source

The screenshot shows the ISMS Search Tool interface. At the top, there is a navigation bar with links for Home, Profile, Password & Security, and Exit. Below this, the breadcrumb 'Source Management > Source List' is visible. A yellow notification banner states 'The source has been activated!'. Below the notification is a table with the following data:

Source ID	Status	Short Name	Full Name	Publisher	Release Date	Operations
1		<a href="#">ISO/IEC 27000:2016</a>	<a href="#">Information technology — Security techniques — Information security management systems — Overview and vocabulary</a>	ISO/IEC JTC 1/SC 27	2016-02-15	

Figure 6.18 A notification after activating a source

The activity diagram which includes all processes of block/unblock source operation is shown in Figure 6.19.



**Figure 6.19** Activity diagram for block/unblock source operations

#### 6.5.3.4 Delete, Recover and Destroy Source Profile

Sources can be deleted from the database when necessary. Due to the principle of work of the relational database, all contents will be deleted when the related source profile is deleted.

A three stage deletion method was constructed to prevent unwanted and irreversible operations. In the first stage, when the delete operation is performed, the source is not actually deleted. This operation changes the status value of the source in the source table to '-1' which means source was deleted. This operation can be undone. After the delete operation, the status icon changed to trash; also undo icon and shred icon is appeared in operation column as seen in Figure 6.20.

ISMS SEARCH TOOL

Home Profile Password & Security Exit

Source Management>Source List

The source has been deleted!

Source ID	Status	Short Name	Full Name	Publisher	Release Date	Operations
1		ISO/IEC 27000:2016	<a href="#">Information technology — Security techniques — Information security management systems — Overview and vocabulary</a>	ISO/IEC JTC 1/SC 27	2016-02-15	
2		ISO/IEC 27001:2013	<a href="#">Information technology — Security techniques — Information security management systems — Requirements</a>	ISO/IEC JTC 1/SC 27	2013-10-01	
3		ISO/IEC 27002:2013	<a href="#">Information technology — Security techniques — Code of practice for information security controls</a>	ISO/IEC JTC 1/SC 27	2013-10-01	

**Figure 6.20** A notification after deleting a source

Later, if it is requested the delete operation can be undone by clicking the recover button located at the right side of the source list. This process re-sets the status value of the source from ‘-1’ to ‘1’.

ISMS SEARCH TOOL

Home Profile Password & Security Exit

Source Management>Source List

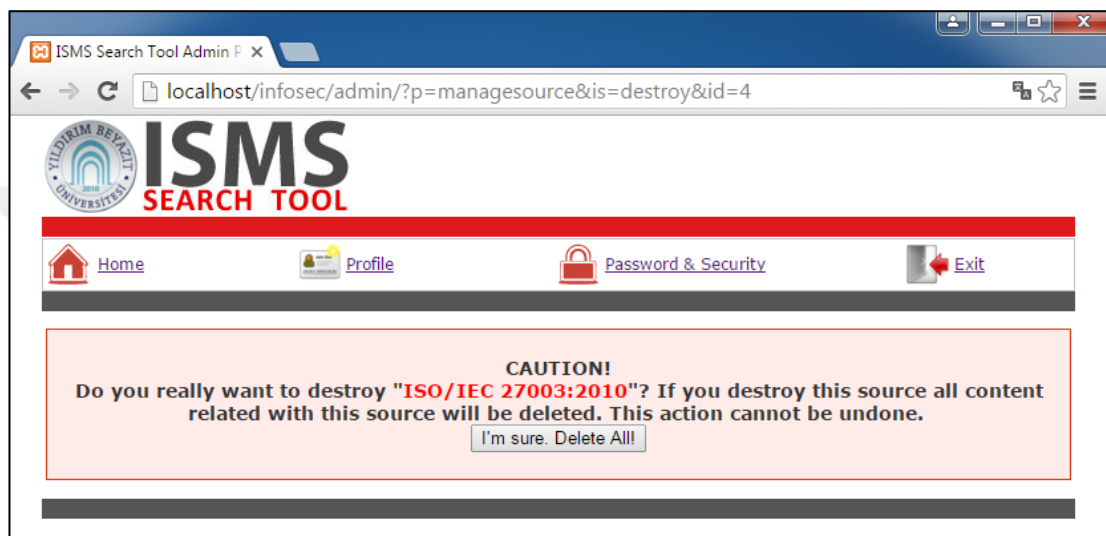
The source has been restored!

Source ID	Status	Short Name	Full Name	Publisher	Release Date	Operations
1		ISO/IEC 27000:2016	<a href="#">Information technology — Security techniques — Information security management systems — Overview and vocabulary</a>	ISO/IEC JTC 1/SC 27	2016-02-15	
2		ISO/IEC 27001:2013	<a href="#">Information technology — Security techniques — Information security management systems — Requirements</a>	ISO/IEC JTC 1/SC 27	2013-10-01	
3		ISO/IEC 27002:2013	<a href="#">Information technology — Security techniques — Code of practice for information security controls</a>	ISO/IEC JTC 1/SC 27	2013-10-01	

**Figure 6.21** Notification message after restore a source

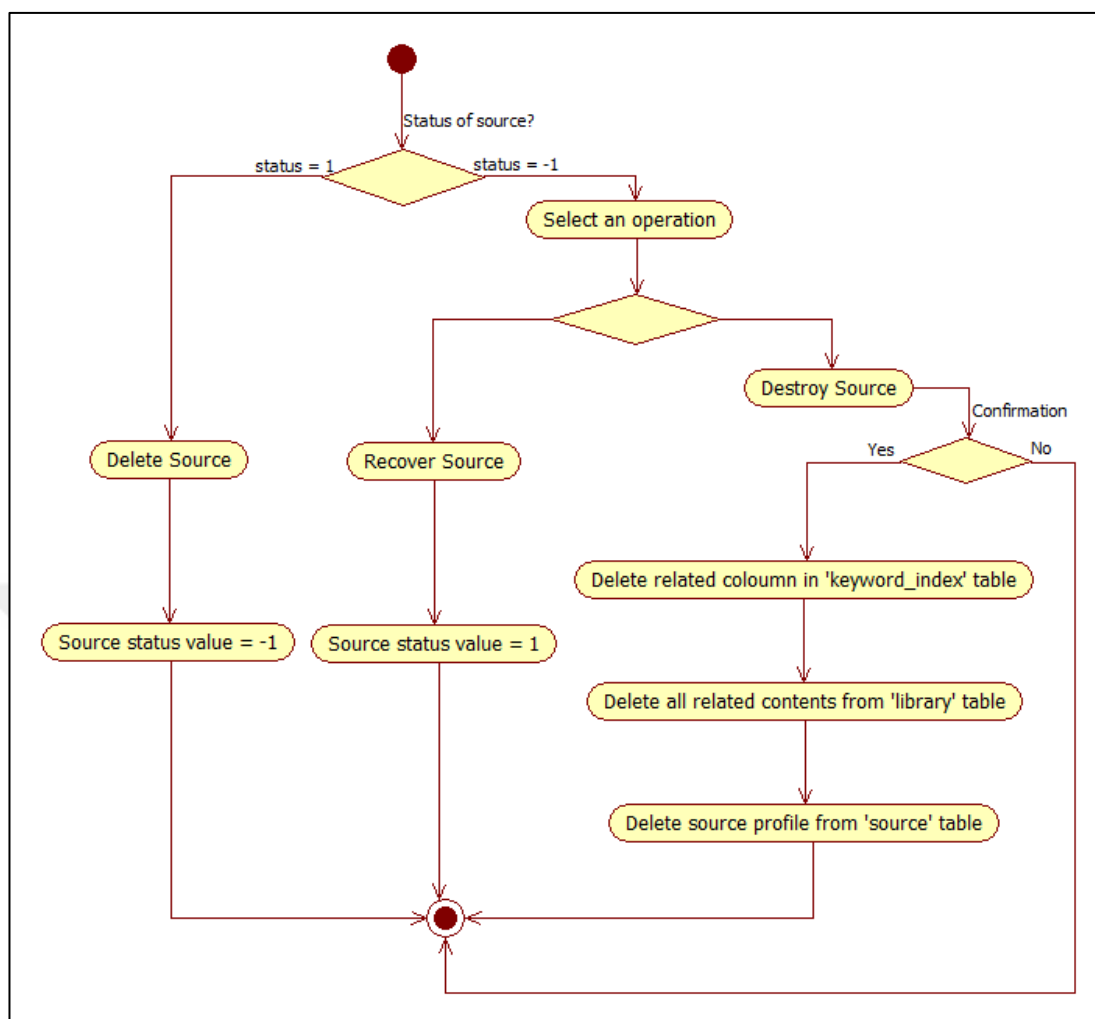
A notification message is displayed as shown in Figure 6.21 at the end of the restore source operation.

If the source is desired to be completely deleted from the database, destroy button is used. This process deletes source profile and all of the contents of the source from database. The destroy operation cannot be reversed so the user is warned as seen in Figure 6.22 before running the process.



**Figure 6.22** Warning message before destroy a source

The activity diagram for delete, recover and destroy source operations are shown in Figure 6.23.




**Figure 6.23** Activity diagram for source management processes

### 6.5.4 Content Management

In the search tool, content means contents of standards which loaded to database. Content management is designed to add, modify and delete the contents of the standard and user can switch the content management section by clicking content management icon in the admin panel.








Authorized users can easily add contents of standards to the database in administration panel. To add contents, the source profile must have been created before which was explained in section 6.5.3.1.





Home Profile Password & Security Exit



Home > Content Management > Select Content

Source ID	Short Name	Full Name	Publisher	Release Date	Select
2	ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements	ISO/IEC JTC 1/SC 27	2013-10-01	
3	ISO/IEC 27002:2013	Information technology — Security techniques — Code of practice for information security controls	ISO/IEC JTC 1/SC 27	2013-10-01	
4	ISO/IEC 27003:2010	Information technology — Security techniques — Information security management system implementation guidance	ISO/IEC JTC 1/SC 27	2010-02-01	
5	ISO/IEC 27004:2009	Information technology — Security techniques — Information security management — Measurement	ISO/IEC JTC 1/SC 27	2009-12-15	
6	ISO/IEC 27005:2011	Information technology — Security techniques — Information security risk management	ISO/IEC JTC 1/SC 27	2011-06-01	
7	ISO/IEC 27006:2015	Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems	ISO/IEC JTC 1/SC 27	2015-10-01	
10	ISO/IEC 27007	Information technology -- Security techniques -- Guidelines for information security management systems auditing	ISO/IEC JTC 1/SC 27	2011-11-15	

**Figure 6.24** Content management main page: list of source

The source list will be appeared given in Figure 6.24 when the content management page is opened. First, source name must be selected by clicking the select icon on the right side of the source list shown in Figure 6.25 to add content. After selecting the source name, a content list will appear shown in Figure 6.26.

Home > Content Management > Select Content

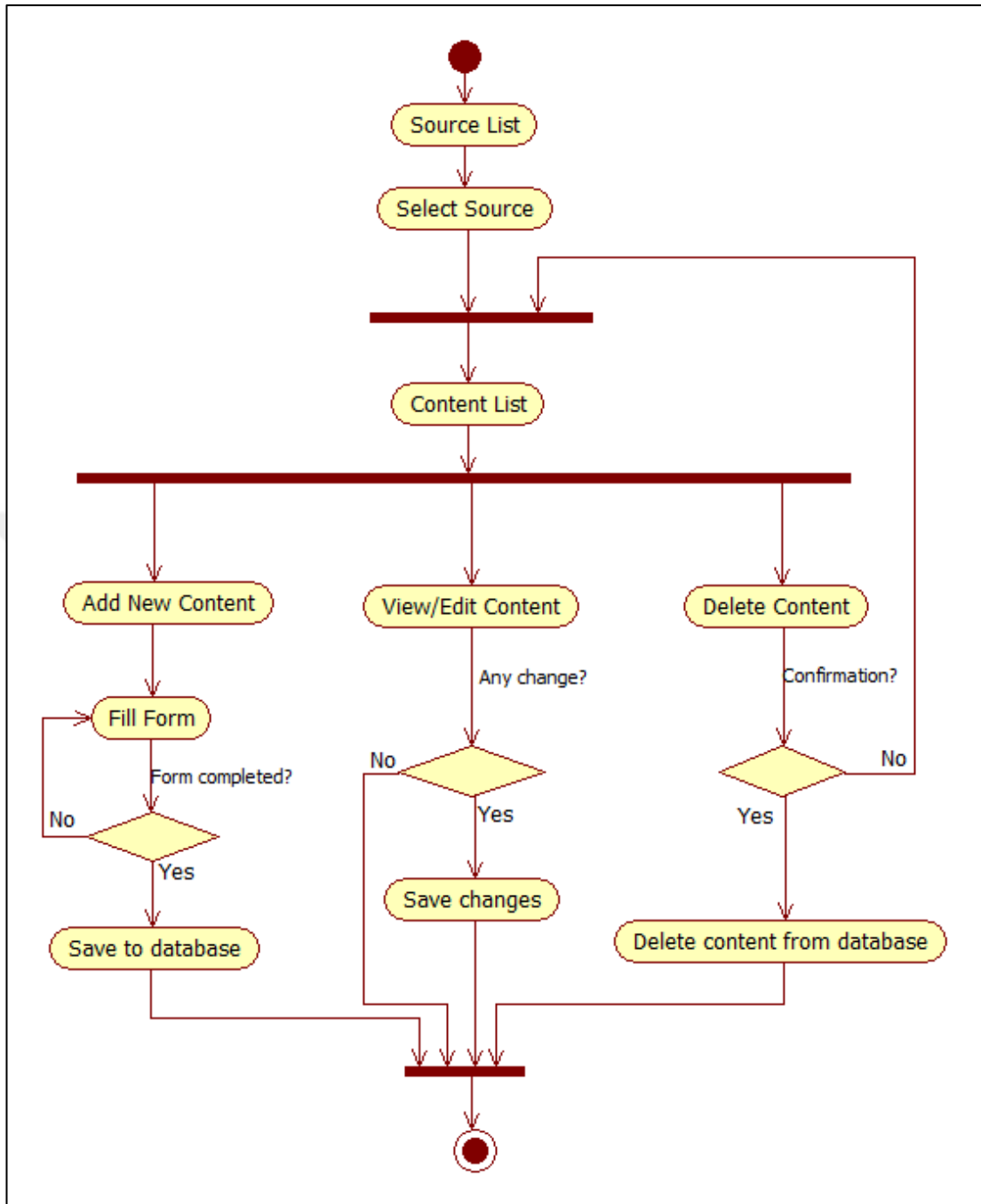
Source ID	Short Name	Full Name	Publisher	Release Date	Select
2	ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements	ISO/IEC JTC 1/SC 27	2013-10-01	
3	ISO/IEC 27002:2013	Information technology — Security techniques — Code of practice for information security controls	ISO/IEC JTC 1/SC 27	2013-10-01	

**Figure 6.25** Selecting a source

Content ID	Title ID	Title	Text	Options
138	0	Introduction		
139	1.1	General	This International Standard has been prepared to provide requirements for establishing, implementi...	
140	1.2	Compatibility with other management system standards	This International Standard applies the high-level structure, identical sub-clause titles, identic...	
141	1	Scope	This International Standard specifies the requirements for establishing, implementing, maintaining...	
142	2	Normative references	The following documents, in whole or in part, are normatively referenced in this document and are ...	
143	3	Terms and definitions	For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply. ...	
144	4	Context of the organization	...	
145	4.1	Understanding the organization and its context	The organization shall determine external and internal issues that are relevant to its purpose and...	
146	4.2	Understanding the needs and expectations of interested parties	The organization shall determine: a) interested parties that are relevant to the information secu...	

**Figure 6.26** Content list for a source

The activity diagram of the whole process of the content management is shown in Figure 6.27. Sub-operations of content management are described in the following titles.



**Figure 6.27** Activity diagram for content management processes

#### 6.5.4.1 Adding New Content

To add new content to the relevant source “Add New Content” button that located top of the content list shown in Figure 6.28 is used. After clicking the button, a new content form as seen in Figure 6.29 is opened. A new content can be added by filling out the fields in the new content form and submitting.

The screenshot shows the ISMS Search Tool interface. At the top, there is a navigation bar with links for Home, Profile, Password & Security, and Exit. Below this, a breadcrumb trail reads: Home > Content Management > ISO/IEC 27001:2013 >. A red box highlights the 'Add New Content' button, with a blue arrow pointing to it from the right. Below the button, the page title is 'Contents of ISO/IEC 27001:2013'. A table lists the contents of the standard:

Content ID	Title ID	Title	Text	Options
138	0	Introduction		
139	1.1	General	This International Standard has been prepared to provide requirements for establishing, implementi...	
140	1.2	Compatibility with other management system standards	This International Standard applies the high-level structure, identical sub-clause titles, identic...	

Figure 6.28 Add new content button

The screenshot shows the 'Add New Content' form in the ISMS Search Tool. The breadcrumb trail is: Home > Content Management > ISO/IEC 27001:2013 > Add New Content. The form has the following fields:

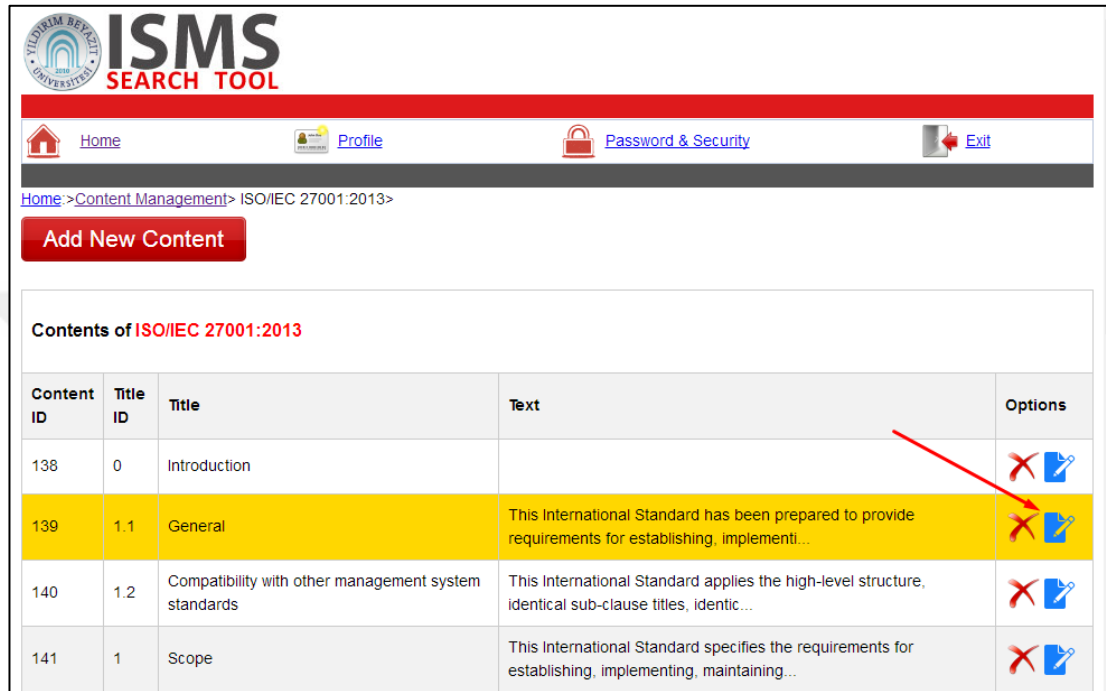
- SOURCE:** A dropdown menu with 'ISO/IEC 27001:2013' selected. A red box with the number '1' is around this field.
- Title Number:** A text input field with 'Last Title Number: 10.2' displayed next to it. A red box with the number '2' is around this field.
- Title:** A text input field.
- Content Text:** A large text area.
- Control:** A text area.
- Implementation Guidance:** A text area.
- Other Information:** A text area.

A 'Submit' button is located at the bottom of the form.









Figure 6.29 New content form

#### 6.5.4.2 View/Edit Content

In this section, content that has been previously added to database can be viewed or edited. Edit content icon must be clicked to open edit form in the related row of the content list as seen in Figure 6.30.



The screenshot displays the ISMS Search Tool interface. At the top, there is a navigation bar with links for Home, Profile, Password & Security, and Exit. Below this, a breadcrumb trail shows the current location: Home > Content Management > ISO/IEC 27001:2013 >. A red button labeled 'Add New Content' is visible. The main content area is titled 'Contents of ISO/IEC 27001:2013' and contains a table with the following data:

Content ID	Title ID	Title	Text	Options
138	0	Introduction		 
139	1.1	General	This International Standard has been prepared to provide requirements for establishing, implementi...	 
140	1.2	Compatibility with other management system standards	This International Standard applies the high-level structure, identical sub-clause titles, identic...	 
141	1	Scope	This International Standard specifies the requirements for establishing, implementing, maintaining...	 

**Figure 6.30** Selecting a content to edit

A form is opened after selecting a content. In this form user can edit or change the content as shown in Figure 6.31. After editing the content changes can be saved to database by clicking the submit button.

**ISMS SEARCH TOOL**

Home Profile Password & Security Exit

Home > Content Management > ISO/IEC 27001:2013

**SOURCE** ISO/IEC 27001:2013

**Title Number** 1.1

**Title** General

**Content Text**  
 This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information

**Control**

**Implementation Guidance**

**Other Information**

Submit

**Figure 6.31** Content view/edit form

#### 6.5.4.3 Remove Content

Content has been previously added to database can be deleted. The process of deleting content is taking in two steps. First step is confirmation and second is deletion from database. After operation is completed it cannot be undone.

To delete content user must select a content in the content list. Delete process can be initiated by clicking the relevant delete icon shown in Figure 6.32. After clicking the delete icon, a notification message will be displayed as seen in Figure 6.33. If the user approves the message, the content will be completely deleted from the database.

**ISMS SEARCH TOOL**

Home Profile Password & Security Exit

Home > Content Management > ISO/IEC 27001:2013 >

**Add New Content**

**Contents of ISO/IEC 27001:2013**

Content ID	Title ID	Title	Text	Options
138	0	Introduction		
139	1.1	General	This International Standard has been prepared to provide requirements for establishing, implementi...	
140	1.2	Compatibility with other management system standards	This International Standard applies the high-level structure, identical sub-clause titles, identic...	
141	1	Scope	This International Standard specifies the requirements for establishing, implementing, maintaining...	
142	2	Normative references	The following documents, in whole or in part, are normatively referenced in this document and are ...	

**Figure 6.32** Deleting a content

**ISMS SEARCH TOOL**

Home Profile Password & Security Exit

Home > Content Management > ISO/IEC 27001:2013 >

Do you really want to delete this content! This action cannot be undone.

**SOURCE ISO/IEC 27001:2013**

**Title Number** 1.2

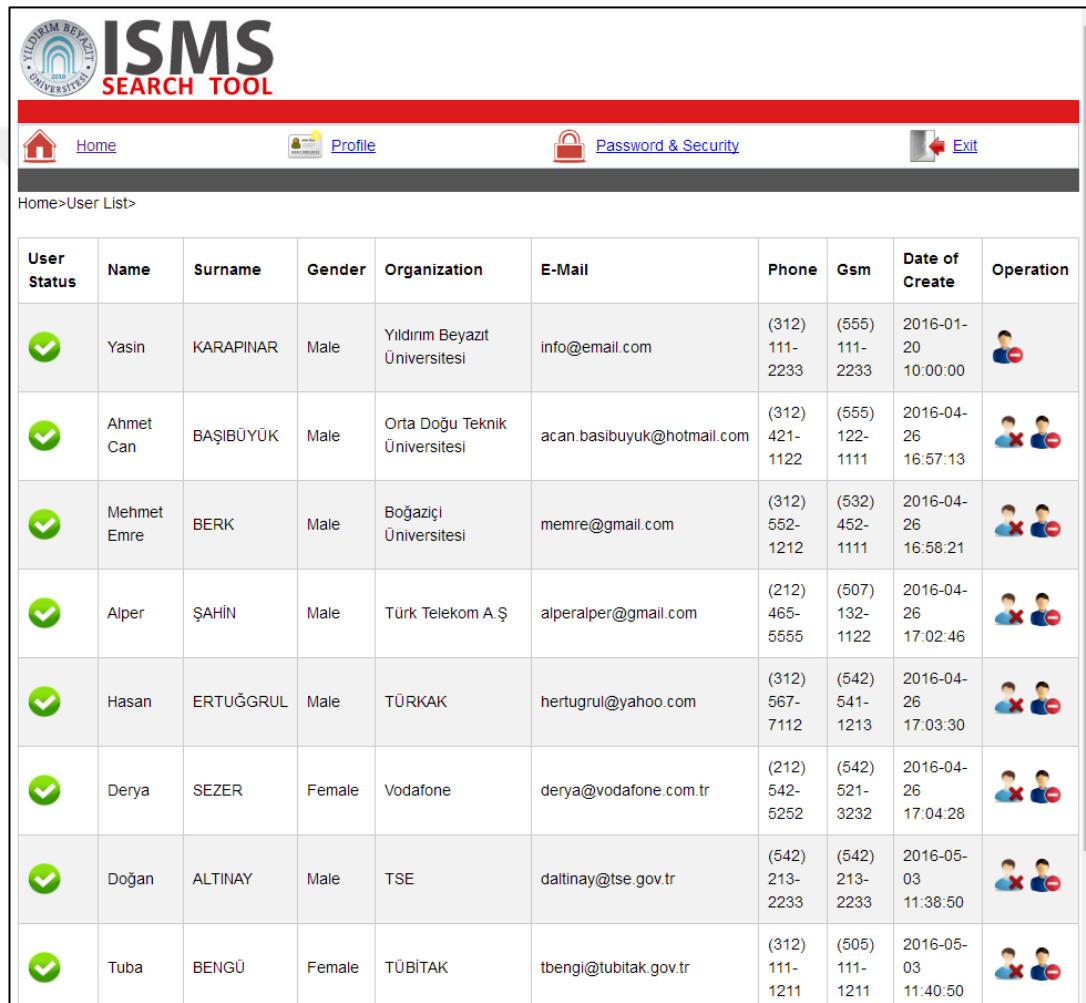
**Title** Compatibility with other management system standards

**Content Text** This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL. This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards. Information technology — Security techniques — Information security management systems — Requirements

**Figure 6.33** Content deletion confirmation message

## 6.5.5 User Management

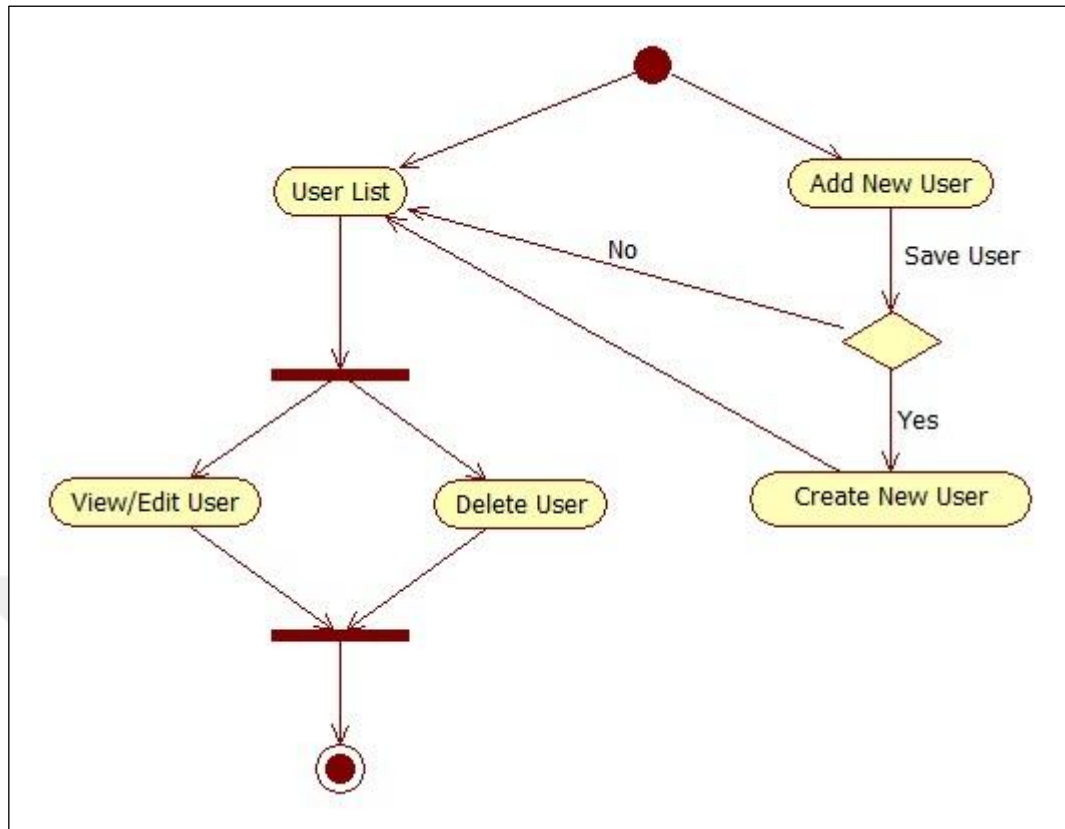
Although it is a part of this search tool, user management is not directly relevant to this thesis study. Due to copyright of standards, the search tool is not open to public so a user authorization mechanism is added to the search tool. On the main page of administration panel user management icon is clicked to switch user management main screen as seen in Figure 6.34. The activity diagram of user management processes is given in Figure 6.35.



User Status	Name	Surname	Gender	Organization	E-Mail	Phone	Gsm	Date of Create	Operation
✓	Yasin	KARAPINAR	Male	Yıldırım Beyazıt Üniversitesi	info@email.com	(312) 111-2233	(555) 111-2233	2016-01-20 10:00:00	
✓	Ahmet Can	BAŞIBÜYÜK	Male	Orta Doğu Teknik Üniversitesi	acan.basibuyuk@hotmail.com	(312) 421-1122	(555) 122-1111	2016-04-26 16:57:13	
✓	Mehmet Emre	BERK	Male	Boğaziçi Üniversitesi	memre@gmail.com	(312) 552-1212	(532) 452-1111	2016-04-26 16:58:21	
✓	Alper	ŞAHİN	Male	Türk Telekom A Ş	alperalper@gmail.com	(212) 465-5555	(507) 132-1122	2016-04-26 17:02:46	
✓	Hasan	ERTUĞRUL	Male	TÜRKAK	hertugrul@yahoo.com	(312) 567-7112	(542) 541-1213	2016-04-26 17:03:30	
✓	Derya	SEZER	Female	Vodafone	derya@vodafone.com.tr	(212) 542-5252	(542) 521-3232	2016-04-26 17:04:28	
✓	Doğan	ALTINAY	Male	TSE	daltinay@tse.gov.tr	(542) 213-2233	(542) 213-2233	2016-05-03 11:38:50	
✓	Tuba	BENGÜ	Female	TÜBİTAK	tbengi@tubitak.gov.tr	(312) 111-1211	(505) 111-1211	2016-05-03 11:40:50	

Figure 6.34 User management screen





**Figure 6.35** Activity diagram for user management processes

#### 6.5.5.1 Adding New User

Administrative users can add a new user to the system. To create a new user first administrator must click create new user button at the bottom of the user list shown in Figure 6.34 and then required form that seen in Figure 6.37 must be filled out. If the form is incomplete or wrongly filled a warning messages appears next to the form fields as shown in Figure 6.38 when form is submitted.

After a submission is completed, an email is sent to the newly created user's e-mail address to inform about the registration and password.

	Derya	SEZER	Female	Vodafone	derya@vodafone.com.tr	(212) 542-5252	(542) 521-3232	2016-04-26 17:04:28	
	Doğan	ALTINAY	Male	TSE	daltinay@tse.gov.tr	(542) 213-2233	(542) 213-2233	2016-05-03 11:38:50	
	Tuba	BENGÜ	Female	TÜBİTAK	tbengi@tubitak.gov.tr	(312) 111-1211	(505) 111-1211	2016-05-03 11:40:50	

[Create New User](#)

**Figure 6.36** Create new user button



# ISMS

## SEARCH TOOL

---

Home
 Profile
 Password & Security
 Exit

---

**Add New User**

Name\*

Surname\*

Gender\*

**Organization Information**

Organization Name\*

Web Address

E-Mail

**Contact Information**

Work Phone\*

GSM \*

**Address Information**

Address

**Figure 6.37** New user form

**ISMS SEARCH TOOL**

Home Profile Password & Security Exit

Home>User List> New User

**Add New User**

Name\* Ahmet  
Surname\* Can  
Gender\* Male

**Organization Information**

Organization Name\* Eskişehir Ormangazi Univ  
Web Address http://esogu.edu.tr  
E-Mail  Required!

**Contact Information**

Work Phone\*  Enter Phone number without begin with 0  
GSM \*  Enter phone number without begin with 0

**Address Information**

Address

Submit

**Figure 6.38** Form validation

#### 6.5.5.2 View/Edit User

User information can be edited and modified. Administrator selects to user by clicking on the line where the user placed and a form with user information is opened shown in Figure 6.39. After changing data form must be submitted and then a notification message will be displayed as seen in Figure 6.39.

**ISMS SEARCH TOOL**

Home Profile Password & Security Exit

**Profile UPDATED Successfully!**

**User Profile**

Name*	Yasin
Surname*	KARAPINAR
Gender*	Male

**Organization Information**

Organization Name*	Yıldırım Beyazıt University
Web Address	http://www.ybu.gov.tr
E-Mail	info@email.com


**Contact Information**

Work Phone*	(312) 111-2233
GSM *	(555) 111-2233

**Figure 6.39** User profile view/edit form

#### 6.5.5.3 Remove User

The delete user icon is located on the right side of the user shown in Figure 6.40 is used to remove user.

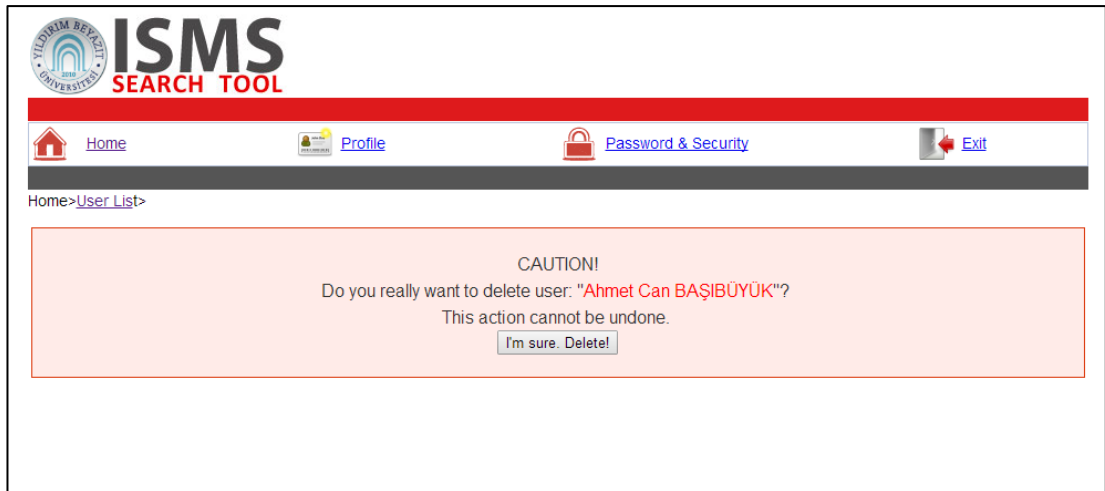


Home > User List >

User Status	Name	Surname	Gender	Organization	E-Mail	Phone	Gsm	Date of Create	Operation
	Yasin	KARAPINAR	Male	Yıldırım Beyazıt Üniversitesi	info@email.com	(312) 111-2233	(555) 111-2233	2016-01-20 10:00:00	
	Ahmet Can	BAŞIBÜYÜK	Male	Orta Doğu Teknik Üniversitesi	acan.basibuyuk@hotmail.com	(312) 421-1122	(555) 122-1111	2016-04-26 16:57:13	
	Mehmet Emre	BERK	Male	Boğaziçi Üniversitesi	memre@gmail.com	(312) 552-1212	(532) 452-1111	2016-04-26 16:58:21	
	Alper	ŞAHİN	Male	Türk Telekom A.Ş.	alperalper@gmail.com	(212) 465-5555	(507) 132-1122	2016-04-26 17:02:46	
	Hasan	ERTUĞRUL	Male	TÜRKAK	hertugrul@yahoo.com	(312) 567-7112	(542) 541-1213	2016-04-26 17:03:30	

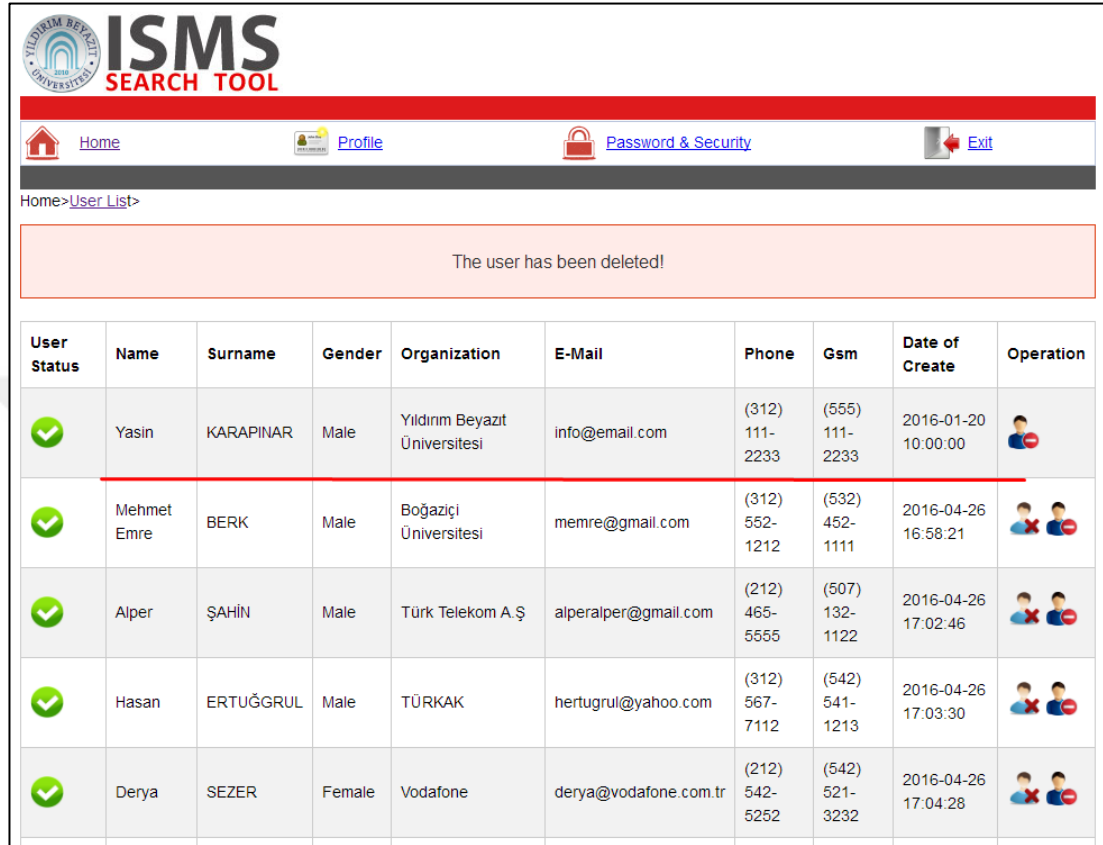
**Figure 6.40** User deletion

After clicking delete user icon, a confirmation message will be displayed as seen in Figure 6.41. If administrator approves the message user is completely deleted from database and this operation is not reverted.



**Figure 6.41** Caution message before deleting a user

After the process is complete, the user information is completely deleted from the database and the user is removed from the list. Then a message shown in Figure 6.42 is displayed that indicates the completion of the process.



The screenshot shows the ISMS Search Tool interface. At the top, there is a navigation bar with links for Home, Profile, Password & Security, and Exit. Below the navigation bar, a message box displays "The user has been deleted!". Below the message box, there is a table with the following columns: User Status, Name, Surname, Gender, Organization, E-Mail, Phone, Gsm, Date of Create, and Operation.

User Status	Name	Surname	Gender	Organization	E-Mail	Phone	Gsm	Date of Create	Operation
✓	Yasin	KARAPINAR	Male	Yıldırım Beyazıt Üniversitesi	info@email.com	(312) 111- 2233	(555) 111- 2233	2016-01-20 10:00:00	
✓	Mehmet Emre	BERK	Male	Boğaziçi Üniversitesi	memre@gmail.com	(312) 552- 1212	(532) 452- 1111	2016-04-26 16:58:21	
✓	Alper	ŞAHİN	Male	Türk Telekom A.Ş.	alperalper@gmail.com	(212) 465- 5555	(507) 132- 1122	2016-04-26 17:02:46	
✓	Hasan	ERTUĞRUL	Male	TÜRKAK	hertugrul@yahoo.com	(312) 567- 7112	(542) 541- 1213	2016-04-26 17:03:30	
✓	Derya	SEZER	Female	Vodafone	derya@vodafone.com.tr	(212) 542- 5252	(542) 521- 3232	2016-04-26 17:04:28	

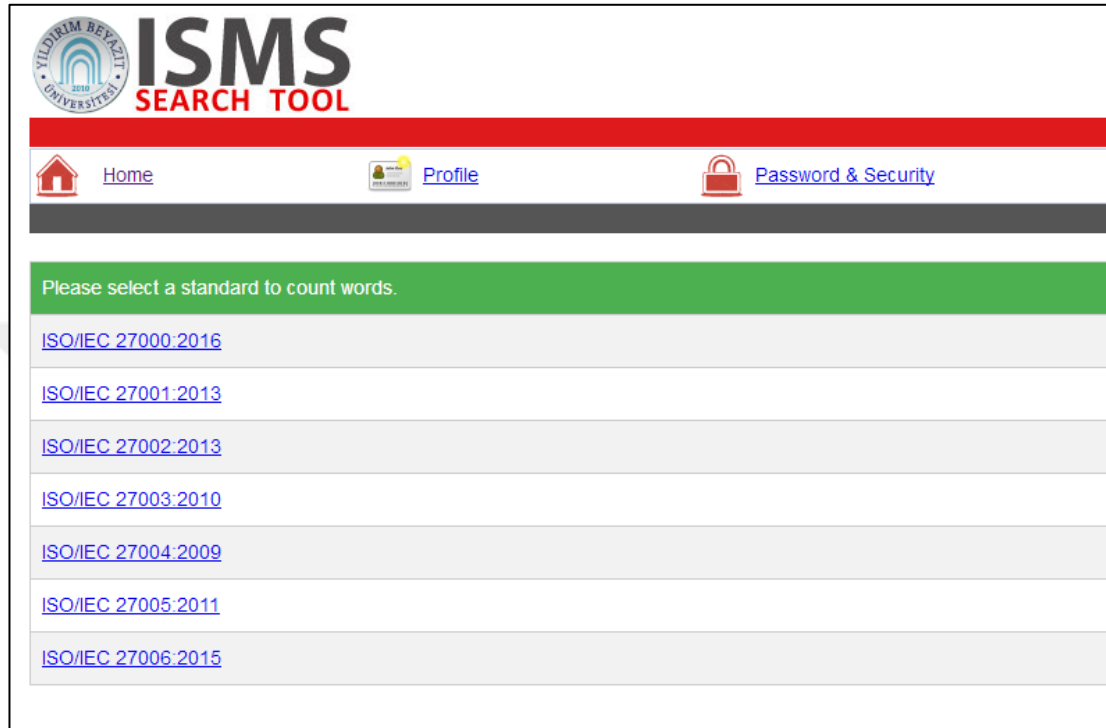
**Figure 6.42** A notification after deleting a user

### 6.5.6 Word Counter

The search tool has a script named “Word Counter” which calculates the frequency of the words used in the standards. Thanks to this tool, users are able to see how many times a word occurs in a specific standard. In return, users can compare the standards in terms of words with each other.

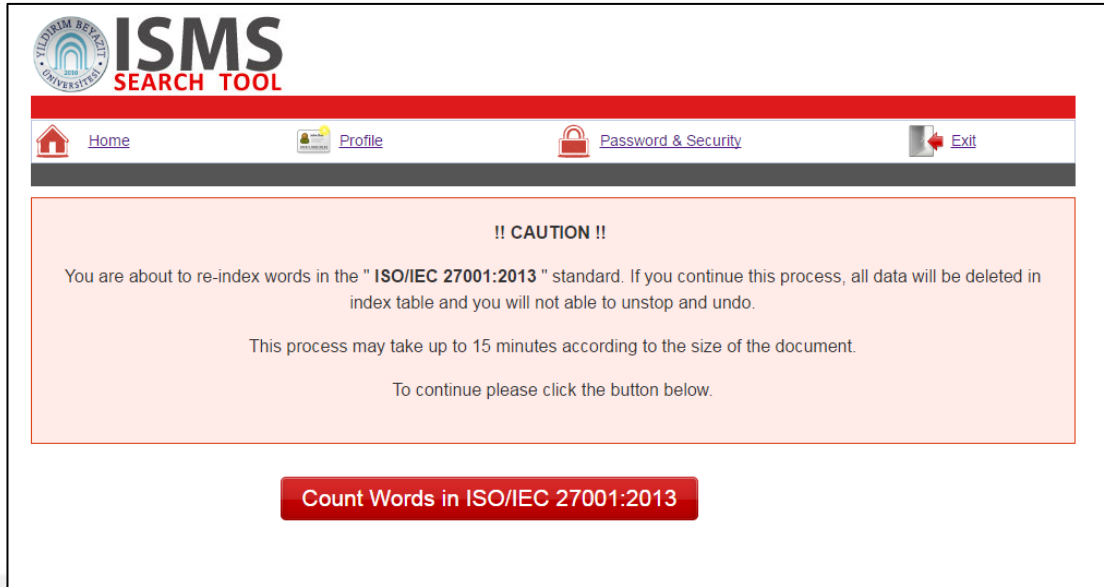
The activity diagram given in Figure 6.45 shows the process of the word counter. This script stores word repetition values in terms of standard name in the ‘word\_index’ table of the database.

On the administrator main page, word counter icon shown is used to navigate to the word counter script page. After clicking the icon, standards that are installed in the database before are listed as seen in Figure 6.43. The administrator can initialize the word counter by clicking the name of the relevant standards in the list.



**Figure 6.43** List of standard in word counter page

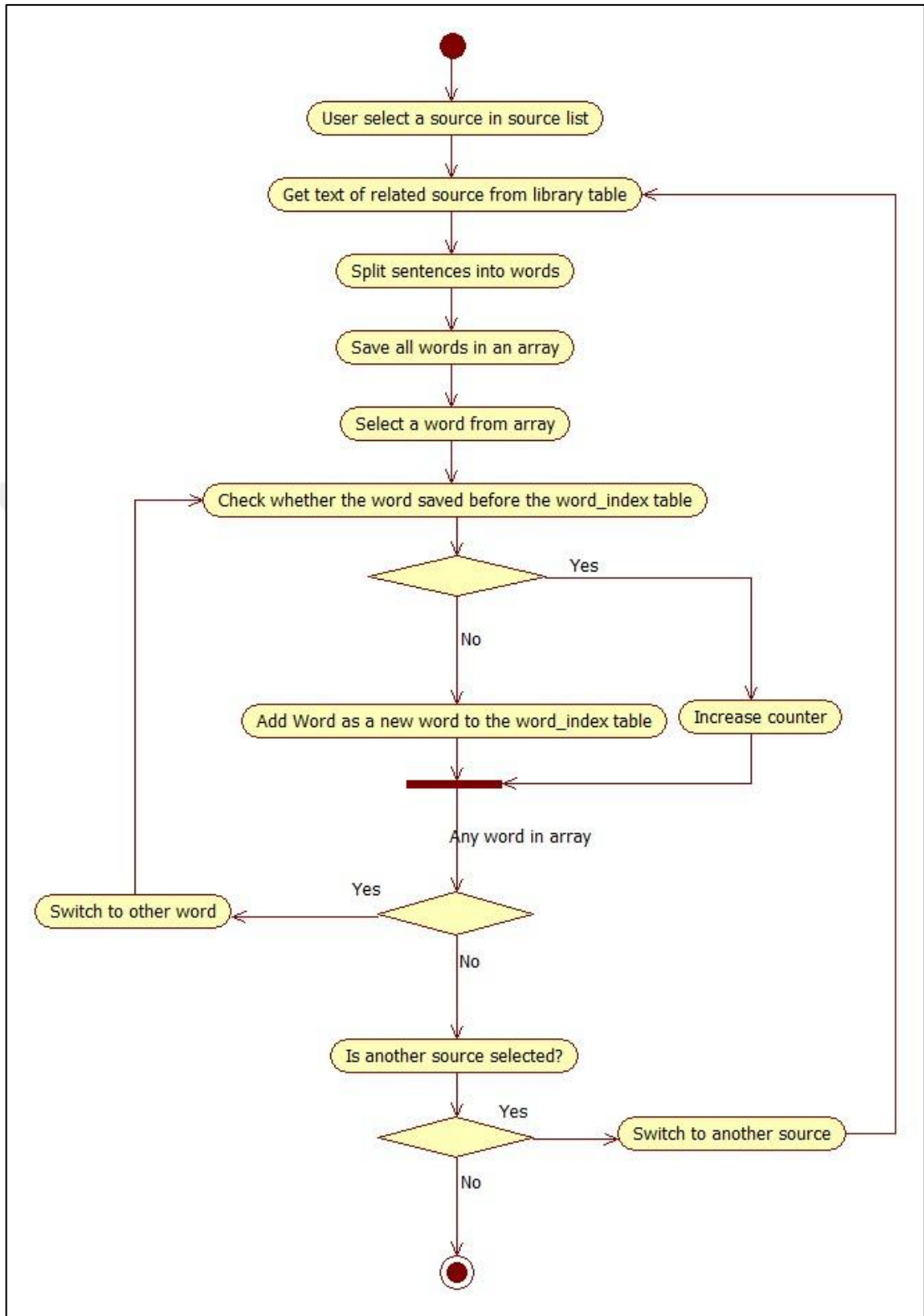
A major warning message is shown in Figure 6.44 that notifies the administrator before running the script because the script first deletes all values from the relevant column of the 'word\_index' table.



**Figure 6.44** Word counter warning message

If the warning seen in Figure 6.44 is accepted, then the script begins to run. First, the script deletes all value in the relevant column and then re-calculates the number of repetition of words in the specified standard.

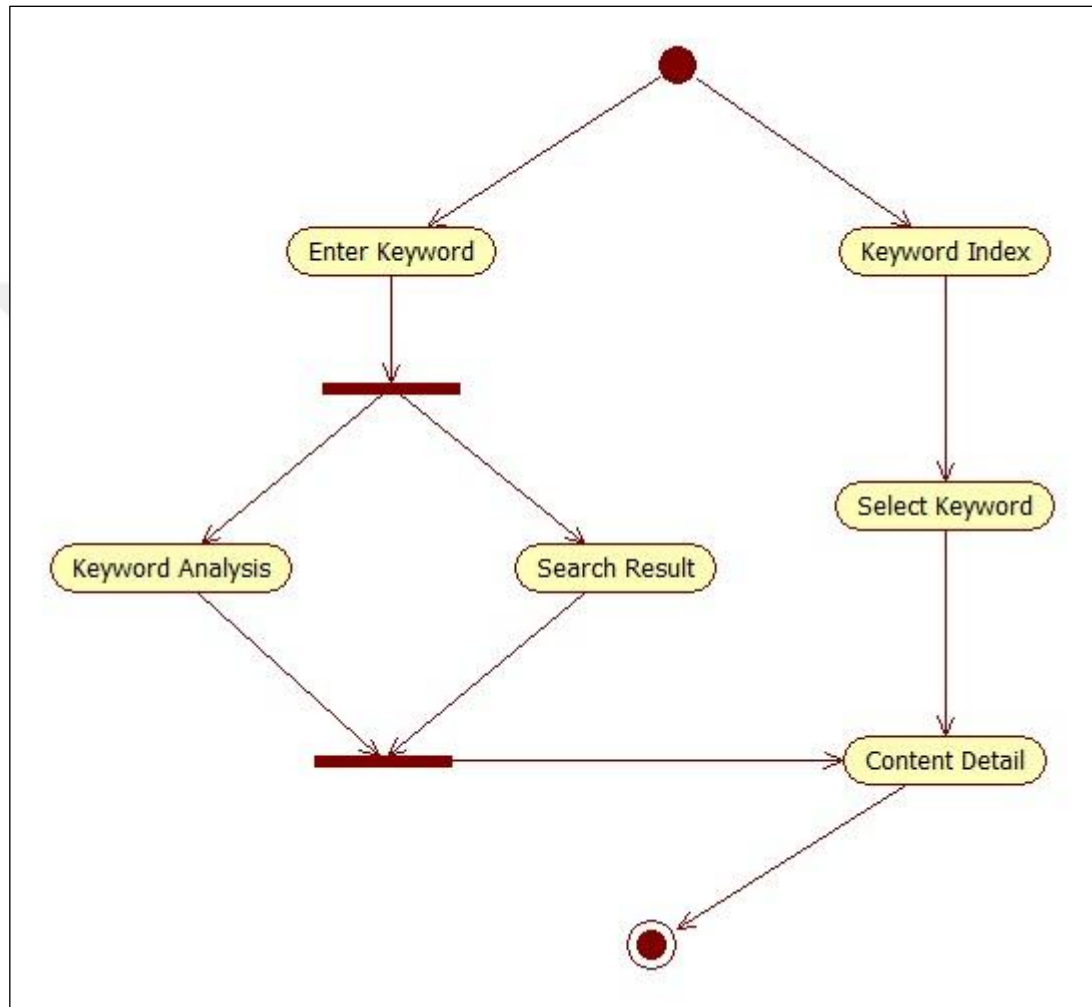




**Figure 6.45** Activity diagram for word counter

## 6.6 End-User Panel

The end-user panel is without a doubt the most important part of the tool. Users can search keywords and analyze standards in this part. The activity diagram describing the processes of the end-user panel is shown in Figure 6.46.



**Figure 6.46** Activity diagram for end-user panel processes

### 6.6.1 End-User Login Page

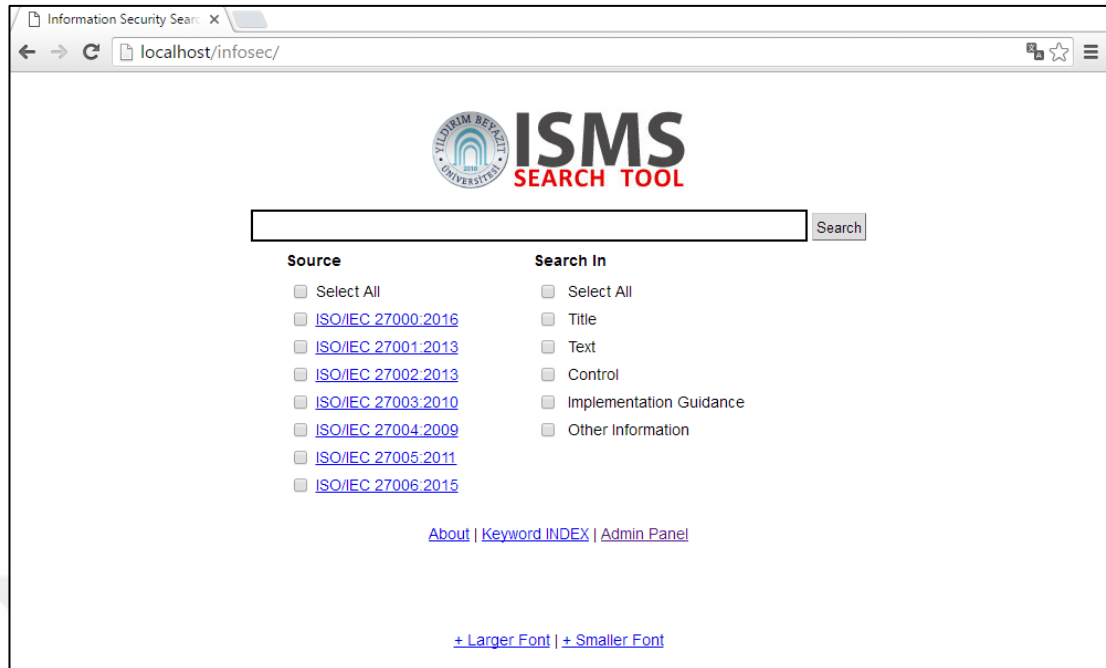
Due to copyright issue of standards, the search tool is not open to the public. Only users who have licenses can access the tool. For this reason, an authentication control and login page is required as seen in Figure 6.47.



**Figure 6.47** End-user login page

### **6.6.2 User Main Page**

The aim for all software designers is for their software have an easy user experience for its users and this search tool is no different. For this reason, the end-user panel has a simple, easy to navigate and straightforward design. The end-user main page shown in Figure 6.48 consists of a search bar, search options and a few links. The search process starts by submitting a keyword in the search bar.



**Figure 6.48** End-user main page

After submitting a keyword, a search query is generated and the query is run on MySQL server. The following steps of the search processes are described in the below sections.

### 6.6.3 Search Query

The most important concept in a keyword search is the query. The keyword must be sought in the most accurate and fastest way throughout the database. This is only possible with an accurately designed database and a well-generated query.

In this search tool, the query consists of two stages. In the first stage the query finds the content where the keyword has occurred. While in second stage, the number of repetitions of the word is calculated.

A sample query generated by the tool is shown in Table 6.1.

Table 6.1 A sample query

```

SELECT ( Length(Lower(`title`)) - Length(
    REPLACE(Lower(`title`), 'information security'
        , '')) ) / ( Length(
        'information security' ) )
AS numOTitle,
( Length(Lower(`text`)) - Length(
    REPLACE(Lower(`text`), 'information security',
        ''
    )) ) / ( Length('information security' ) ) AS
numOText,
( Length(Lower(`control`)) - Length(
    REPLACE(Lower(`control`), 'information security', '')
) ) / ( Length(
    'information security' ) )
AS numOControl,
( Length(Lower(`implementation_guidance`)) - Length(
    REPLACE(Lower(`implementation_guidance`), 'information
security', ''))
) / (
    Length('information security' ) )
AS numOImGui,
( Length(Lower(`other_information`)) - Length(
    REPLACE(Lower(`other_information`), 'information
security', '')) ) / (
    Length(
        'information security' ) )
AS numOInfo,
+( Length(Lower(`title`)) - Length(
    REPLACE(Lower(`title`), 'information security'
        , '')) ) / ( Length('information security' ) ) + (
    Length(Lower(`text`)) - Length(
        REPLACE(Lower(`text`), 'information security', ''
    )) ) / ( Length('information security' ) ) + (
        Length(Lower(`control`)) - Length(
            REPLACE(Lower(`control`), 'information security', '')) )
) / ( Length(
    'information security' ) ) + (
    Length(Lower(`implementation_guidance`))
        - Length(
            REPLACE(Lower(`implementation_guidance`),
                'information security',
                '')) ) / ( Length(
                'information security' ) ) + (
                Length(Lower(`other_information`)) - Length(
                    REPLACE(Lower(`other_information`), 'information
security'
                    , '')) ) / ( Length('information security' ) )
AS sumOTotal,
library.*,
source.short_name
AS source_name,
source.id
AS source_id

```

**Table 6.1** A sample query (continuation)

```

FROM library
LEFT JOIN source
ON library.source = source.id
WHERE title LIKE '% information security%'
      OR title LIKE 'information security%'
      OR title REGEXP '[[:<:]]information security\[[:>:]]'
      OR text LIKE '% information security%'
      OR text LIKE 'information security%'
      OR text REGEXP '[[:<:]]information security\[[:>:]]'
      OR control LIKE '% information security%'
      OR control LIKE 'information security%'
      OR control REGEXP '[[:<:]]information security\[[:>:]]'
      OR implementation_guidance LIKE '% information
security%'
      OR implementation_guidance LIKE 'information security%'
      OR implementation_guidance REGEXP '[[:<:]]information
security\[[:>:]]'
      OR other_information LIKE '% information security%'
      OR other_information LIKE 'information security%'
      OR other_information REGEXP '[[:<:]]information
security\[[:>:]]'
AND ( +( Length(Lower(`title`)) - Length(
REPLACE(Lower(`title`), 'information security', '')) ) / (
Length('information security') ) + (
Length(Lower(`text`)) - Length(
REPLACE(Lower(`text`), 'information security', ''
)) ) / ( Length('information security') ) + (
Length(Lower(`control`)) - Length(
REPLACE(Lower(`control`), 'information security'
, '')) ) / ( Length('information security') ) + (
Length(Lower(`implementation_guidance`)) - Length(
REPLACE(Lower(`implementation_guidance`), 'information
security', '')) ) / ( Length('information security') ) + (
Length(Lower(`other_information`))
- Length( REPLACE(Lower(`other_information`),
'information security', '')) ) / ( Length('information security'
) ) ) > 0
ORDER BY source ASC,
library.id ASC

```

#### 6.6.4 Search Result

After the query runs, a result page is generated as seen in Figure 6.49. The table on the result page given in Figure 6.50 shows the number of repetitions of the keyword in the standards. In addition, topics with heading numbers are listed which include the keyword and the number of repetition is indicated in the parenthesis on the same line.

A graphic is also generated shown in Figure 6.51 on the result page for users to compare the standards in terms of searched keywords.

Information Security Search: X  
 localhost/infosec/?act=search&kw=security

**ISMS SEARCH TOOL**

security

Title
  Text
  Control
  Implementation Guidance
  Other Information

ISO/IEC 27000:2014
  ISO/IEC 27001:2013
  ISO/IEC 27002:2013
  ISO/IEC 27003:2010
  ISO/IEC 27004:2009
  ISO/IEC 27005:2011
  ISO/IEC 27006:2015

Standard Name	Repetition
ISO/IEC 27000:2014	185
ISO/IEC 27001:2013	105
ISO/IEC 27002:2013	440
ISO/IEC 27003:2010	185
ISO/IEC 27004:2009	115
ISO/IEC 27005:2011	101
ISO/IEC 27006:2015	69
<b>Total</b>	<b>1200</b>

**Keyword Analysis**  
 The frequency of repetition of the word 'security'

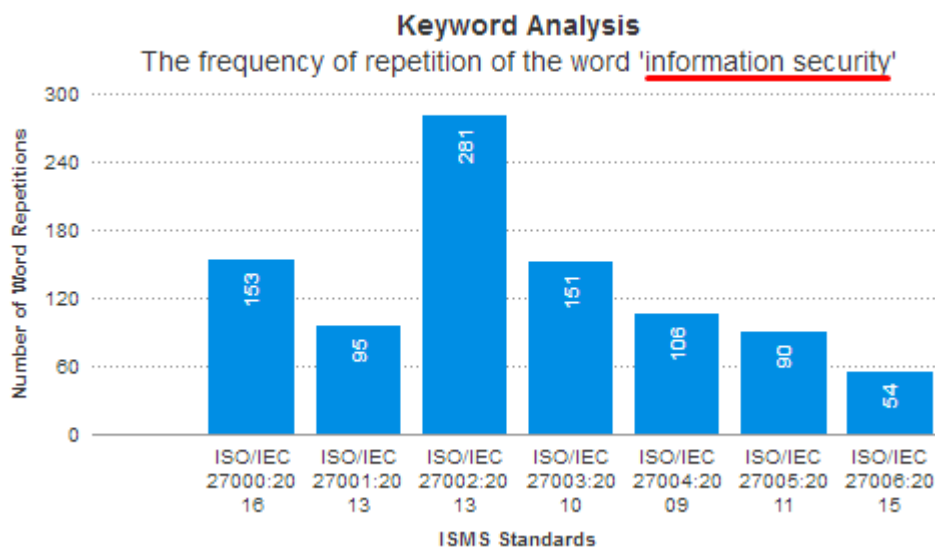
ISO/IEC 27000:2014 (185)

- [0.1 Overview](#) (3)
- [0.2 ISMS family of standards](#) (18)
- [0.3 Purpose of this International Standard](#) (1)
- [1 Scope](#) (1)
  - [2.1 access control](#) (1)
  - [2.14 consequence](#) (1)
  - [2.28 governance of information security](#) (2)
  - [2.33 information security](#) (1)
  - [2.34 information security continuity](#) (2)

Figure 6.49 Search result page

Standard Name	Repetition
ISO/IEC 27000:2016	153
ISO/IEC 27001:2013	95
ISO/IEC 27002:2013	281
ISO/IEC 27003:2010	151
ISO/IEC 27004:2009	106
ISO/IEC 27005:2011	90
ISO/IEC 27006:2015	54
<b>Total</b>	<b>930</b>

**Figure 6.50** Keyword repetition table



**Figure 6.51** Keyword frequency graphic

When any of the titles that are listed on the results page is clicked, the content opens as seen in Figure 6.52. In the content page, the searched keyword is highlighted.



The screenshot displays the ISMS SEARCH TOOL interface. At the top left is the logo of Yıldırım Beyazıt University. The main header contains a search bar with the text 'information security' and a 'Search' button. Below the search bar are several filter options: 'Title', 'Text', 'Control', 'Implementation Guidance', and 'Other Information'. A row of checkboxes allows users to select specific ISO/IEC standards: 27000:2016 (checked), 27001:2013, 27002:2013, 27003:2010, 27004:2009, 27005:2011, and 27006:2015.

The main content area is titled 'ISO/IEC 27000:2016' and includes a navigation menu on the left with the following items:


- 0 Introduction
- 1 Scope
- 2 Terms and definitions
- 3 Information security management systems
  - 3.1 Introduction
  - 3.2 What is an ISMS?
    - 3.2.1 Overview and principles
    - 3.2.2 Information
    - 3.2.3 Information security
    - 3.2.4 Management
    - 3.2.5 Management system
  - 3.3 Process approach
  - 3.4 Why an ISMS is important
  - 3.5 Establishing, monitoring, maintaining and improving an ISMS
  - 3.6 ISMS critical success factors
  - 3.7 Benefits of the ISMS family of standards
- 4 ISMS family of standards

The main content area is titled '3.2.3 Information security' (ISO/IEC 27000:2016). The text describes the dimensions of information security: confidentiality, availability, and integrity. It states that information security involves the application and management of appropriate security measures to ensure sustained business success and continuity. It further explains that information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using an ISMS, including policies, processes, procedures, organizational structures, software, and hardware to protect information assets. These controls need to be specified, implemented, monitored, reviewed, and improved where necessary to ensure that specific information security and business objectives are met. Relevant information security controls are expected to be seamlessly integrated with an organization's business processes.

Figure 6.52 Content page

### 6.6.5 Keyword Index

The keyword index page shown in Figure 6.53 provides information for the user about the words that have been found in the standards. On this page, users can get a quick overview of the last words in the standards. At the top of the word list, standard names are located as tabs. Each standard is sorted in their own tabs that can be clicked individually. Words can either be sorted alphabetically or based on frequency with a simple click of a sort button on the top of the table.



# ISMS

SEARCH TOOL

Title
  Text
  Control
  Implementation Guidance
  Other Information

ISO/IEC 27000:2016
  ISO/IEC 27001:2013
  ISO/IEC 27002:2013
  ISO/IEC 27003:2010
  ISO/IEC 27004:2009
  ISO/IEC 27005:2011
  ISO/IEC 27006:2015

---

### Word Index & Their Count

Sort: A Z 0 9

ISO/IEC 27000:2016
  ISO/IEC 27001:2013
  ISO/IEC 27002:2013
  ISO/IEC 27003:2010
  ISO/IEC 27004:2009
  ISO/IEC 27005:2011
  ISO/IEC 27006:2015

Frequency of Word (DESC) <span style="float: right;">→</span>					
<a href="#">should</a> (796)	<a href="#">information</a> (730)	<a href="#">security</a> (440)	<a href="#">that</a> (226)	<a href="#">access</a> (224)	<a href="#">organization</a> (221)
<a href="#">with</a> (210)	<a href="#">controls</a> (165)	<a href="#">requirements</a> (157)	<a href="#">management</a> (155)	<a href="#">procedures</a> (154)	<a href="#">system</a> (120)
<a href="#">systems</a> (117)	<a href="#">software</a> (100)	<a href="#">business</a> (98)	<a href="#">other</a> (98)	<a href="#">from</a> (97)	<a href="#">control</a> (95)
<a href="#">such</a> (89)	<a href="#">protection</a> (84)	<a href="#">ensure</a> (81)	<a href="#">when</a> (81)	<a href="#">appropriate</a> (79)	<a href="#">services</a> (78)
<a href="#">their</a> (74)	<a href="#">assets</a> (74)	<a href="#">changes</a> (73)	<a href="#">this</a> (72)	<a href="#">policy</a> (72)	<a href="#">considered</a> (70)
<a href="#">data</a> (67)	<a href="#">user</a> (66)	<a href="#">process</a> (64)	<a href="#">which</a> (64)	<a href="#">users</a> (64)	<a href="#">where</a> (63)
<a href="#">external</a> (62)	<a href="#">responsibilities</a> (62)	<a href="#">rights</a> (62)	<a href="#">processing</a> (61)	<a href="#">media</a> (61)	<a href="#">secure</a> (61)
<a href="#">equipment</a> (61)	<a href="#">following</a> (59)	<a href="#">network</a> (59)	<a href="#">risk</a> (58)	<a href="#">development</a> (57)	<a href="#">unauthorized</a> (57)
<a href="#">facilities</a> (56)	<a href="#">used</a> (56)	<a href="#">operational</a> (56)	<a href="#">processes</a> (55)	<a href="#">required</a> (55)	<a href="#">supplier</a> (55)
<a href="#">also</a> (54)	<a href="#">relevant</a> (54)	<a href="#">including</a> (52)	<a href="#">testing</a> (52)	<a href="#">policies</a> (51)	<a href="#">service</a> (51)
<a href="#">authentication</a> (50)	<a href="#">review</a> (48)	<a href="#">have</a> (47)	<a href="#">include</a> (46)	<a href="#">classification</a> (45)	<a href="#">physical</a> (44)
<a href="#">they</a> (44)	<a href="#">cryptographic</a> (44)	<a href="#">need</a> (43)	<a href="#">into</a> (43)	<a href="#">implemented</a> (43)	<a href="#">agreements</a> (43)

**Figure 6.53** Keyword index page

# CHAPTER 7

## FUTURE WORK AND CONCLUSION

### 7.1 Future Work

Certain aspects of the search tool designed in this thesis may be improved in several ways. For instance, this search tool can be transformed and developed into a modular ISMS application with an add-on system. Some of these suggested add-ons are listed below;

- PDF or DOC document importer: The most time consuming thing in the tool is loading standards to the database manually. To minimize this, a module can be developed which can automatically import document from PDF or DOC format to the database.
- ISMS implementation project estimator: By collecting specific parameters from an organization, the estimator calculates the timescale needed to implement the chosen ISMS standard.
- ISMS implementation plan: A structured starter plan and schedule to expand and be ameliorate the chosen ISMS to suit the organization.
- ISMS implementation tracker: A combined status tracker for the mandatory ISMS and optional security controls in ISO/IEC 27001:2013. Statement of applicability and gap analysis, used to track progress of the ISMS implementation project towards certification and more.
- ISMS mandatory documentation checklist: An advanced guide to the documentation and records formally required or recommended for certification for ISO/IEC 27001:2013.

## 7.2 Conclusion

In today's technology, the importance of information is constantly increasing and in turn is becoming a valuable asset for all organizations big or small, commercial or nonprofit.

Keeping this in mind, at present, information must be accessible at anytime and anywhere therefore information technologies are designed in accordance with this requirement and this requirement brings with it some problems. In other words; networks, systems, servers, computers are designed to be able to access the information on demand which also makes information open to threats. As mentioned above, the importance and basic concepts of information security have been explained in detail throughout CHAPTER 2.

Consequently, various institutions have established the IT-based information security standards in order to protect information that is considered an important and critical asset for organizations. Although these standards are similar, they also have differences in some aspects that have been explained in CHAPTER 3.

Even though there many institutions with their own versions of ISMS standards, the world's most preferred standard for information security management by organizations is ISO/IEC 27000 family of standards which is developed by the International Electrotechnical Commission and Subcommittee SC 27 of ISO (the International Organization for Standardization). There are currently 36 standards that belong to this family, within these standards nine of them are in the preparation phase and haven't been published yet. Detailed information about ISO/IEC 27000 family of standards have been given in CHAPTER 4.

Under these circumstances, the number of ISMS standards that information security professionals and auditors need to work with have increased considerably. To solve this problem that has occurred from the flood of these standards, a search tool for information security standards has been designed and developed in this thesis to help IT professionals and auditors alike.

A dynamic web-based programming technique was used in order to develop the search tool. Additionally, a server based three-layered software architecture approach was taken for this tool as well as a relational database model was chosen for the database design. The general concepts of software and database design selected for the tool have been presented in CHAPTER 6.

A sample study was conducted by loading certain standards of ISO/IEC 27000 family of standards to the developed search tool. After loading standards to the tool, some keywords were searched to check the functionality of the tool. It was observed that the tool works with high accuracy. In depth implementation details of the tool have also been provided in CHAPTER 6.

After a keyword was searched, a table was generated on the result page. In this table, the standard name is shown followed by the repetition number. Thus, users are able to see and compare easily which of the standards referred to the keyword more frequently.

Within the admin panel, the tool also has a built in word counter section. Once executed, this option counts and indexes all words within the standards. Therefore, the end user is able to see all the words with its number of frequencies. Once a word has been chosen, a table and graph is generated for the user to compare the standards repetition results.

Due to the nature of the growing ISMS industry, the tool being scalable is an important advantage to have so any number of new standards can be installed. It is also not standard specific, meaning not only ISO standards can be installed but also other published standards by different institutes can be loaded in to the tool.

Ultimately, in this thesis a search tool was developed for information security standards by using a three-layered, database linked and web-based dynamic software technique. A tested version of this tool has been designed, implemented and executed successfully by loading the first seven standards of ISO/IEC 27000 family of standards.

## REFERENCES

- [1] ISO, “*ISO - International Organization for Standardization* [Online]”, Geneva, Web: <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> [29.11.2014].
- [2] ISO/IEC, “*ISO 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary*”, ISO, Geneva, 2014.
- [3] Eremba Ltd., “*About Us | eramba - open-source IT GRC* [Online]”, London, Web: <http://www.eramba.org/about> [07.05. 2016].
- [4] SerNet GmbH, “*Verinice Product* [Online]”, Göttingen, Web: <https://verinice.com/en/product> [07.05.2016].
- [5] Neupart, “*SecureAware ISMS-tool* [Online]”, Scottsdale, Web: <http://www.neupart.com/products/isms-package> [07.05.2016].
- [6] Biznet Bilisim, “*ISMart* [Online]”, İstanbul, Web: <http://www.biznet.com.tr/en/ismart/> [07.05.2016].
- [7] National Institute of Standards and Technology, US Department of Commerce., “*Guide for Applying the Risk Management Framework to Federal Information Systems*”, Special Publication, Gaithersburg, 2010.
- [8] Bundesamt für Sicherheit in der Informationstechnik, BSI., “*Federal Office for Information Security* [Online]”, Bonn, Web: [https://www.bsi.bund.de/EN/TheBSI/thebsi\\_node.html](https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) [01.05.2016].
- [9] Bundesamt für Sicherheit in der Informationstechnik, “*BSI-Standard 100-1: Information Security Management Systems (ISMS)*”, BSI, Bonn, 2008.
- [10] Bundesamt für Sicherheit in der Informationstechnik, “*BSI-Standard 100-3 Risk analysis based on IT-Grundschutz*”, BSI, Bonn, 2008.
- [11] ISACA, “*Introduction to Cobit 5* [Online]”, Rolling Meadows, Web: <http://www.isaca.org/Education/Upcoming-Events/Documents/Intro-COBIT5.pdf> [4.12.2015].
- [12] IT Governance Institute, “*Cobit 4.1 Excerpt Executive Summary Framework*”, ITGI, Illinois, 2007.

- [13] ISACA, “*About COBIT 5 / What is COBIT / Management Framework – ISACA* [Online]”, Web: <https://cobitonline.isaca.org/about> [4.12.2015].
- [14] Tipton, Harold F. and Krause, Micki., “*Information Security Management Handbook, Sixth Edition, Volume 2*”, Auerbach Publications, New York, 2008.
- [15] Bidgoli, Hossein., “*Handbook of Information Security Vol.3 Threats, Vulnerabilities, Prevention, Detection and Management.*”, John Wiley & Sons Inc., New Jersey, 2006.
- [16] US Department of Commerce National Institute of Standards and Technology, “*NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*”, U.S. Department of Commerce, Gaithersburg, 2013.
- [17] CERT Division of the Software Engineering Institute (SEI), Carnegie Mellon University., “*Cyber Risk and Resilience Management* [Online]”, Pittsburgh, Web: <http://www.cert.org/resilience/products-services/octave/> [11.05.2016].
- [18] Open Group, “*About The Open Group* [Online]”, Berks, Web: <http://www.opengroup.org> [12.05.2016].
- [19] The Open Group, “*Open Group Standard - Open Information Security Management Maturity Model (O-ISM3)*”, The Open Group, Berkshire, 2011.
- [20] Risk Assessment Special Interest Group (SIG), PCI Security Standards Council., “*Information Supplement: PCI DSS Risk Assessment Guidelines*”, PCI Security Standards Council, 2012.
- [21] ISO, “*ISO/IEC 27001 - Information security management* [Online]”, Geneva, Web: <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> [05.05.2016].
- [22] ISO/IEC, “*ISO/IEC 27001:2005 Information technology -- Security techniques - Information security management systems – Requirements*”, ISO, Geneva, 2005.
- [23] ISO/IEC, “*ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance*”, ISO, Geneva, 2010.
- [24] ISO/IEC, “*ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement*”, ISO, Geneva, 2009.

- [25] ISO, “*ISO/IEC 27005:2011 - Information technology — Security techniques — Information security risk management*”, ISO, Geneva, 2011.
- [26] ISO, “*ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*”, ISO, Geneva, 2015.
- [27] PHP, “*PHP Manual [Online]*”, Cary, Web: <http://php.net/manual/en/intro-what-is.php> [17.01.2016].
- [28] MySQL, “*MySQL 5.7 Reference [Online]*”, Redwood Shores, Web: <http://dev.mysql.com/doc/refman/5.7/en/what-is-mysql.html> [17.02.2016].
- [29] Netcraft, “*April 2016 Web Server Survey [Online]*”, Bath, Web: <http://news.netcraft.com/archives/2016/04/21/april-2016-web-server-survey.html> [17.05.2016].
- [30] Rouse, Margaret., “*What is Web server [Online]*”, Newton, Web: <http://whatis.techtarget.com/definition/Web-server>, [15.05.2016]
- [31] Eftaiha, Diana., “*An Introduction to Apache [Online]*”, Melbourne, Web: <http://code.tutsplus.com/tutorials/an-introduction-to-apache--net-25786> [16.05.2016].
- [32] Codd, Edgar Frank., “*Derivability, Redundancy, and Consistency of Relations Stored in Large Data Banks*”, IBM Research Report, California, 1969.



# RESUME

## Personal Information

Name and Surname : Yasin KARAPINAR

Date of Birth : 05.01.1984

Place of Birth : Kırıkkale

## Education

- B.Sc., Electrical-Electronics Engineering, Eskişehir Osmangazi University, Eskişehir, 2003-2008.
- High School, Science, Çankırı Süleyman Demirel Fen Lisesi, Çankırı, 1999-2002.

## Professional Experiences

- Transport Network Specialist, Türk Telekomunikasyon A.Ş, Ankara, 2008-2016.
- Mobile Network Optimization Engineer, LCC Ltd, Ankara, July-November 2008.