ÇANKAYA UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
MATHEMATICS AND COMPUTER SCIENCE

MASTER THESIS

A PROTOTYPE FOR ASSESSMENT OF INFORMATION SECURITY AWARENESS AND IMPLEMENTATION LEVEL

Meltem KOCAMUSTAFAOĞULLARI

JUNE 2013

Title of the Thesis : A Prototype for Information Security Awareness and Implementation Level

Submitted by Meltem KOCAMUSTAFAOĞULLARI

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

Prof. Dr. Taner ALTUNOK
Director

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

Prof.Dr. Billur KAYMAKÇALAN
Head of Department

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

Prof. Dr. Taner ALTUNOK
Supervisor

Examination Date : **6.June.2013**

Examination Committee Members

Prof.Dr. Taner ALTUNOK (Çankaya Univ.)

Prof.Dr. Mehmet Reşit TOLUN (TED Univ.)

Yrd.Doç.Dr. Murat SARAN (Çankaya Univ.)

STATEMENT OF NON-PLAGIARISM PAGE

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

Name, Last Name : Meltem KOCAMUSTAFAOĞULLARI

Signature :

Date : June 2013

ABSTRACT

A PROTOTYPE FOR ASSESSMENT OF INFORMATION SECURITY AWARENESS AND IMPLEMENTATION LEVEL

KOCAMUSTAFAOĞULLARI, Meltem
M.Sc, Department of Information Technology
Supervisor: Prof.Dr. Taner ALTUNOK

June 2013, 135 pages

Information is one of the most valuable assets for any organization and it should always be appropriately protected. Information security is the protection of information against threats to ensure the business continuity. Relying only on the technology is not sufficient and the human factor is the weakest cycle which needs to be strengthened for effective and sustainable information security management. Information security is not only related with technology but it is rather harmonization of people processes and technology. Organizations have the tendency to take action after security incident occurs instead of proactively. There is lack of awareness concerning the information security concepts and its necessity. Awareness and understanding at management level is utmost important to establish and maintain security culture in the organization.

Organizations should be aware of information security aspects, understand their own security requirements and implement countermeasures accordingly. There are good practices and internationally accepted security standards such as ISO/IEC 27001 and ISO/IEC 27002 that can be taken as reference point and guidance. Organizations should establish and implement, sustain and improve information security management taking into account the proven good practices tailored for their own requirements.

In this thesis it has been aimed;

i. To provide a prototype model and tool for self assessment of information security awareness and implementation level of organizations,
ii. To provide a tool to utilize as reference point for organization in building own security requirements and objectives as well as monitoring own overall progress,
iii. To facilitate a self explanatory web-based tool addressing wide range of users without the need for prior training or in-depth technical knowledge on information security based on ISO/IEC 27001 and ISO/IEC 27002 international security standards and covering essential and common practice security topics,
iv. To provide comparable values with other organizations who have similar information security requirements,
v. To prepare tool in Turkish for contributing to improvement of information security awareness and implementation among organizations.

The model is designed in eight sections for assessment of; IS Corporate Approach, Information Assets Security, Human Resources Security, Physical and Environmental Security, Communications and Information Systems Operations, Information Systems Access Control, Development and Maintenance Management, IS Incident Management and Business Continuity, IS Compliance and Monitoring Management. The tool is implemented in line with the designed model and tested by experts having solid professional background on information security as well as selective users in Turkey from various sectors such as finance, public authorities, consulting companies and education. The feedback and results verified that the objectives of the thesis are achieved and the tool can serve to improve information security awareness and implementation level of the target users with its web based, self explanatory and user friendly tool environment.

Keywords: Information Security, Information Security Management Assessment, Information Security Awareness Level, ISO/IEC 27001, Information Security Implementation Level, Information Security Management Benchmark, Prototype Model for Information Security Management Assessment, Prototype Tool for Information Security Management Assessment.

ÖZ

BİLGİ GÜVENLİĞİ FARKINDALIĞI VE UYGULAMA SEVİYESİ DEĞERLENDİRMEK İÇİN BİLGİ GÜVENLİĞİ PROTOTİP UYGULAMASI

KOCAMUSTAFAOĞULLARI, Meltem
Yüksek Lisans, Bilgi Teknolojileri Anabilim Dalı
Tez Yöneticisi: Prof.Dr. Taner ALTUNOK

Haziran 2013, 135 sayfa

Bir organizasyon için bilgi en kıymetli varlıklarından biridir ve uygun şekilde korunmalıdır. Bilgi güvenliği, iş sürekliliğinin sağlanabilmesi için bilginin tehtitlere karşı korunmasıdır. Bu amaçla, yalnız teknolojiye güvenmek yeterli değildir çünkü insan faktörü bilgi güvenliğindeki en zayıf halkadır. Bilgi güvenliği yönetiminin verimli olması ve sürekliliğinin sağlanması için insan faktörünün bilinçlendirilmesi önemlidir. Bilgi güvenliği yalnız teknolojiyle ilintili olmayıp, insan, süreç ve teknolojinin birlikte entegre ve uyumu ile gerçekleştirilebilir. Organizasyonlar genelde öncesinden önlem almak yerine, bilgi güvenliği olayı başgösterdiğinde harekete geçme eğilimindedirler. Bilgi güvenliği hususları ve gerekliliğinde farkındalığın arttırılmasına ihtiyaç vardır. Özellikle, yönetim seviyesindeki kişilerin farkındalık ve anlayışı, kurum bilgi güvenliği kültürü oluşturulması açısından önemlidir. Organizasyonlar bilgi güvenliği hususlarında bilinçlenmeli, kendi güvenlik ihtiyaçlarını belirlemeli ve buna göre gerekli önlemlerini almalıdırlar. Bu amaçla geliştirilmiş ve uluslararası kabul görmüş ISO/IEC 27001 ve ISO/IEC 27002 gibi standartlar mevcuttur. Organizasyonlar bu standartları referans noktası ve rehber olarak alabilir ve kendi ihtiyaçlarına uygun olarak, bilgi güvenliği yönetimi sistematiği oluşturarak, sürdürebilir ve gerekli iyileştirmeleri yapabilirler.

Bu tez çalışmasında amaçlanan;

i. Organizasyonların bilgi güvenliği farkındalık ve uygulama seviyelerine yönelik kendi öz değerlendirilmelerini yapabilmeleri için prototip bir model ve araç sağlamak,
ii. Organizasyonların kendi bilgi güvenliği gereksinim ve amaçlarını belirlerken ve gelişmelerini izlerken referans noktası olarak kullanabilecekleri bir araç sağlamak,
iii. Öncesinde eğitim veya detay teknik bilgi gerektirmeden geniş bir kullanıcı kesimine hitap edebilmek, ISO/IEC 27001 and ISO/IEC 27002 bilgi güvenliği standartlarını temel alan, temel bilgi güvenliği hususlarını kapsayan, kolay kullanımlı web tabanlı bir araç sağlamak,
iv. Benzeri bilgi güvenliği ihtiyaçları olan diğer kurumlar ile karşılaştırma yapabilecek şekilde değerler sunmak,
v. Bilgi güvenliği farkındalık ve uygulamaların iyileştirilmesine katkı sağlayabilmek için Türkçe bir araç hazırlamak.

Model sekiz bölümde değerlendirme yapılabilecek şekilde tasarlanmış olup bölümler şunlardır; Bilgi Güvenliği Kurumsal Yaklaşım, Bilgi Kaynakları Güvenliği, İnsan Kaynakları Güvenliği, Fiziksel ve Çevresel Güvenlik, İletişim ve Bilgi Sistemleri İşletimi, Bilgi Sistemleri Erişim Kontrolü, Geliştirme ve Bakım Yönetimi, Bilgi Güvenliği Olay Yönetimi ve İş Sürekliliği, Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi. Bu modele uygun şekilde geliştirilmiş olan araç, bilgi güvenliği konularında kayda değer ve sektörel tecrübeleri olan uzmanlar ve finans, kamu, danışmanlık ve eğitim sektörlerinden seçkin kullanıcılar tarafından test edilmiştir. Geri bildirim ve sonuçlar göstermektedir ki; tezin amaçlarına ulaşılmış ve bu araç, hedef kullanıcı kitlesinin farkındalık ve uygulama seviyesine katkıda bulunabilecek ve ihtiyaç olunan; web tabanlı, açık ve anlaşılır, kolay kullanımlı bir ortam sunmaktadır.

Anahtar Kelimeler: Bilgi Güvenliği, Bilgi Güvenliği Yönetimi Değerlendirme, Bilgi Güvenliği Farkındalık Seviyesi, ISO/IEC 27001, Bilgi Güvenliği Uygulama Seviyesi, Bilgi Güvenliği Yönetimi Karşılaştırma, Bilgi Güvenliği Yönetimi Değerlendirilmesi için Prototip Model, Bilgi Güvenliği Yönetimi Değerlendirilmesi için Prototip Araç.

ACKNOWLEDGEMENTS

The author wishes to express her deepest gratitude to her supervisor Prof.Dr. Taner ALTUNOK for his valuable guidance and advice, his insight and encouragements throughout this study. The author would like to convey her appreciation to Prof.Dr. Billur KAYMAKÇALAN.

The author would also like to extend her gratitude to Mrs. Aslı DOĞRUSÖZ, founding partner of Invento, Mrs. Müjgan ÇETİN from Yeditepe University and Mr.Serdar BİTİK from TÜV SÜD Türkiye, for their comments, recommendations and provision of valuable knowledge as expert views.

The author gratefully acknowledges technical assistance and support of Mr. Ali Özkan ÖZEREN as founding partner of AGEM and Mr. Kemal KOCAMUSTAFAOĞULLARI as founding partner of KMO Information Systems

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

BS	British Standards
BSI	British Standards Institute
COBIT	Control Objectives for Information and related Technology (Bilgi & İlgili Teknolojiler İçin Kontrol Hedefleri)
HW	Hardware
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
IS	Information Security
ISMART	Information Security Management Software developed by BizNet Cooperation (Türkiye)
ISMS	Information Security Management System (ISMS)
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/ International Electro technical Commission
ICT	Information Communication Technology
IT	Information Technology
ITIL	Information Technology Infrastructure Library
OECD	The Organization for Economic Cooperation and Development
PDCA	Plan-Do-Check-Act
QMS	Quality Management System
SME	Small Medium Enterprises
SW	Software
TSE	Turkish Standards Institute (Türk Standartları Enstitüsü)

CHAPTER I

INTRODUCTION

Information is one of the most valuable assets for any organization. As work environment becomes more dependent on the information communication technology (ICT) infrastructure and evolving web based technologies, the security of information asset becomes more and more important.

According to ISO/IEC 17799:2005(E) international standard, information can exist in many forms such as; on paper or in electronic environment, can be presented in slide or film or can be transferred by electronic media. Whatever the form information takes or in what format it is shared or stored, it is evident that information should always be appropriately protected. Information security is the protection of information from a wide range of threats, in order to ensure business continuity and minimize business risk and maximize the business benefits. [1]

No matter the size or type, any organization should first become aware and realize the need for information security and understand that it should be managed similar the other organizational processes. After identifying their own security requirements, organization should plan and execute a practical roadmap to systematically implement and maintain the security of their information assets. Good practices and standards have been developed, in order to guide the organizations in how to establish and manage their information security.

While the availability and accessibility of the information is crucial, at the same time the confidentiality and privacy of the data is highly important. The loss or leakage of information should be taken care of preventively and systematically. When information security is concerned, relying only on the utilization of technology itself may not be sufficient. Building and sustaining a corporate level information security

understanding, culture and advocacy are utmost important. Insider threats (either willingly or unwillingly) are considerably high in comparison to external threats mainly due to lack of awareness.

However among any, the initial step is that the organization needs to be aware and understand what information security is, assess and identify its status and own security requirements. The management level may not be aware or have correct understanding and ownership of the concept of information security. The nature of the organization's business can require different level of security requirements. For example; organization hosting personal information subject to data privacy would require higher level of security then others (i.e. banks, telecommunication companies, public bodies). Organization needs to appropriately reflect necessary security measures to organizational strategies and policies as well as integrate with the business processes. Organization should establish and implement, sustain and improve information security management tailored for own needs.

International standards and best practices on information security can provide good basis for the organizations. ISO/IEC 27001:2005 provides a model for all types of organizations for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The requirements set out in this standard are intended to be applicable to all organizations including private enterprises and government agencies. Organizations can benefit this standard by taking it as reference and tailoring to their own needs.[2].

Organizations can utilize assessment or guidance methods that are based on the international information security standards to assess and understand their awareness and implementation level in information security management. Outcome of such assessment can be used as basis to build organizational security strategies and take corrective actions accordingly. Organization can then use ISO/IEC 27001:2005 as roadmap, adopt and implement in compliance with its strategy and specific requirements.

Organizations have the tendency not to proactively invest in information security management but to initiate action after a security incident occurs or due to legal and regulatory compliance requirements. The main reason behind is the lack of awareness of the information security concepts and its necessity. General miss-approach is also to think information security is related only with information technologies and should be left to the technical staff. Even if the technical staff is aware of its necessity and acts to implement, it is not enough without having the ownership and understanding at all levels of management as well as organizational strategy with harmonization of people, processes and technology.

But even if organization is willing, it often may not know where to start. Organization needs a starting point to first assess its own status and identify its weaknesses regarding information security management. Options can be; referencing international standards and best practices, having consulting services to assess the current status or utilize assessment method or tool. Identifying own information security requirements and referencing and adopting ISO/IEC 27001:2005 international standard is one of the best approaches to address the security challenges. All of these will require financial investment and commitment of human resources.

A reliable and simple facility that is based on ISO/IEC 27001:2005 would be useful for organization to make their own assessment without requirement of initial financial investment or prior training pre-requisite. Also to gain initial understanding of their weaknesses or overall level and even understand their status in comparison to other organizations with similar security requirements. Such assessment can even serve for the purpose of management awareness and ownership.

With the ownership of its management, if organization can make initial self assessment in order to identify the level of its own information security implementation, it can set the basis for the next steps. Organization can establish policy and procedures enabling information security to become as integral part of corporate business processes.

Organizations need be aware of where they stand with at least basic level of understanding of their status in terms of their information security requirements and implementation. Not necessarily to get certification or compliance but to protect their valuable assets and reputation as well as business continuity.

The objectives of this thesis are;

i. To provide a prototype model and tool for self assessment of information security awareness and implementation level of organizations.
ii. To provide a tool to utilize as reference point for organization in building own security requirements and objectives as well as monitoring own overall progress.
iii. To facilitate a self explanatory web-based tool addressing wide range of users without the need for prior training or in-depth technical knowledge on information security based on ISO/IEC 27001 and ISO/IEC 27002 international security standards and covering essential and common practice security topics.
iv. To provide comparable values with other organizations who have similar information security requirements
v. To prepare tool in Turkish for contributing to improvement of information security awareness and implementation among organizations.

This Thesis is organized as the following;

Chapter 1 provides introductory information including; background and problem issues on information security and the objective of this thesis.

Chapter 2 includes related research on information security including; its main concepts, information security related threats and the concept of information security management system to control and minimize such threats. Widely known best practices and standards on IS management more specifically focusing on ISO/IEC 27001 and ISO/IEC 27002 and adaptation to these standards. Case reviews on IS management are given followed by research related to IS awareness and implementation level assessment.

Chapter 3 provides the purpose and scope of IS awareness and implementation level assessment followed by main assumptions and dependencies identified, modeling approach and steps to the modeling based on security standards and expert consultation in establishment of the benchmarking aspect of the model.

Chapter 4 covers the key factors to the model and prototype application, design and implementation steps of the prototype ISM awareness and implementation level assessment tool, identification of test users, test and utilization of the tool with the test users and compile the test results and evaluation of the results.

This thesis finalizes with conclusion, notes for future work and references.

CHAPTER II

LITERATURE SURVEY

During the literature survey, the following have been focused and examined; main issues about information security, two main international security standards which are closely related with each other, aspects and adaptation steps for information security management system to handle information security view on the current status with various survey and case reviews, information security awareness and implementation level assessment or guidance models to support organizations in understanding and improving their level of information security management practices and countermeasures.

2.1. INFORMATION SECURITY

International security standards define an asset as anything that has value to the organization which can be in variety of forms such as; information, software assets, physical assets, people with their qualifications-skills-experience, reputation or image of the organization, etc. Information is one of the most important assets since it is knowledge or data that has value to the organization. [3]

Information needs to be protected in appropriate manner. It can have various definitions;

- Processed Data with added value (i.e. bid evaluation results in a public authority, exam results in education organization, etc.)
- Asset to; produce, pass over, procure, sell, use/consume. It provides power to its owner (i.e. chemical mixture formula for a product, bank account code, investment budget, software design-source code)
- Valuable resource for the organization (i.e. citizen information in database of a public authority)

Information can be in different forms including; digital (electronic, magnetic), material (paper, printout), as knowledge of staff. Information can be presented or shared by various means; in real or virtual environment, electronically, verbally, via courier etc.

As also stated in the ISO/IEC 27002, code of practice for information security management, organizations may be different in nature or size but they all collect, process, store, and transmit information.[3] In order to operate efficiently; it is important that authorized access is available in due time to accurate and complete information. Today's organizations rely heavily on Information Communication Technologies (ICT) and in many respects it is essential for the organization's operational conduct. ICT technologies and tools are used in all the phases of; creation, processing, storing, transmitting, protection, destruction of information. Hybrid work environment is used including but not limited to; intranet – extranet, remote access, mobile communication.

Protecting valuable information assets against any threats and vulnerabilities is utmost important for any organization. Organization needs to take necessary precautions, in order to prevent damage to its assets or image.

According to ISO/IEC 27001, internationally recognized standard for information security management systems – requirements, information security can be defined as "preservation of confidentiality, integrity and availability of information". [2] The main dimensions of information security are; Confidentiality, Availability and Integrity.

i. Confidentiality can be preserved as the information is made available or disclosed only to authorized individuals, entities, or processes. [2] (i.e. Who has access to my personnel information?)
ii. Availability can be preserved with information being accessible and usable upon demand by an authorized entity. [2] (i.e. Is up-to-date exchange information available at time of need?)
iii. Integrity can be preserved provided that the accuracy and completeness of the information is protected. [2] (i.e. Does my bank statement details reflect the actual transactions?)

2.2. INFORMATION SECURITY THREATS AND MANAGEMENT

Threat is defined in ISO/IEC 27002 as “a potential cause of an unwanted incident, which may result in harm to a system or organization”. [1]

A threat has the potential to harm assets such as information, processes and systems. Threats may be of natural or human origin, and could be accidental or deliberate. Organizations should be aware that due to dynamic business environment (change in information systems, utilized technology infrastructures, etc.) relevant threats can also continuously change accordingly.

Utilization and dependency on technology together brings the possibility of related threats and risks to information and their management. The need of security is raised from many reasons including protection to avoid threats such as;

- Possible data losses, data leakage
- Attacks (phishing, buffer overflow, IP spoofing, packet replay, etc.)
- Miss-utilization of personal identification
- Malicious software threats (virus, worm, Trojan, spam, hoax, etc.)
- Social engineering

Threats are not limited only with technology. Human factor is the weakest cycle in the information security. Organization should protect its information assets not only to external threats but also against internal threats.

Some samples for information security threats can be listed as:

- Negligent staff (unattended computer, critical information on post-it, etc.)
- Skipping protection-security steps due to urgency-speed
- Lack of reporting security violations
- Lack of installing latest version-patches of software
- Employees who misuse / miss-configure system security functions
- Unauthorized access, modification or disclosure of information assets
- Cyber-criminals, hackers, malware, trojans, phishes, spammers
- Technical advances that can render encryption algorithms obsolete
- Storms, tornados, floods

Some samples for information security impacts as result of realization of security threats can be listed as:

- Disruption to organizational routines and processes
- Disruption of plans and deadlines
- Financial losses through information theft and fraud
- Loss of confidence in IT
- Reputation damage, loss of business value
- Expenditure on IS asset and data damaged, stolen, corrupted or lost
- Loss of competitive advantage
- Loss of privacy
- Injury or loss of life if safety-critical systems fail

As defined in ISO/IEC 27002; vulnerability is “a weakness of an asset or group of assets that can be exploited by one or more threats”. [1] The presence of vulnerability does not cause harm by itself and a threat needs to be present to exploit it. Weakness may occur due to relevant threats in different part(s) of the cycle; physical environment, system-network infrastructure, information system configuration, process and procedures, management, personnel, software application, communications equipment, etc.

Due to modern IT environment evolving in complexity and interdependency, threats and vulnerabilities are becoming increasingly difficult to address. Organizations rely on mobile devices which facilitate convenience for productivity in the workplace but at the same time will continue to be a source of various types of security incidents. Increased use of social media and use of employee’s own device introduce growing number of threats. Although cloud computing is one of the key emerging technologies, reliability and security is still a concern. The privacy and data protection is serious concern and challenge. Threats over personal information and breaches in data protection can lead to reputational risk as well as interruptions in operation. Governments all around the world are stepping up their regulatory efforts to protect their citizens with information security regulations and legislation.

Firewalls, antivirus software, intrusion detection systems, sophisticated patch management and periodic vulnerability scanning programs are not sufficient to cover

and manage the evolving range of security risks. Proper information security management and risk management should be applied and security controls should be implemented to minimize the related risks. It is vital important to identify and prevent issues before they arise and organization to be prepared to manage the unexpected situations.

According to ISO/IEC 27002, “Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties.” [1]

Key factors that require consideration under IS management include;

- Policies and procedures
- Training and awareness
- Privacy and data protection strategy
- Organization wide inventory of information assets
- Security integrated into operational business activities
- Monitoring for ongoing assurance

Human factor is the weak circle of the organizational security and critical factor for its improvement starting with initial and continuous awareness and monitoring. In most cases, senior management is not aware or recognizes the extent of the security risks to the organization. For sustainable and effective organizational security culture, awareness and ownership must be achieved at all levels of management.

2.3. INFORMATION SECURITY MANAGEMENT SYSTEM

Organization can ensure the continuity of operation, achieve its objectives and maintain its obligatory compliance (if any) by establishing systematic approach to protect information assets including; planning, implementing, maintaining and

improving information security effectively. Elements of information security management include such coordinated activities and implementing suitable controls and treating information security risks. [3]

Information Security Management System (ISMS) is not a technological process. It is rather a systematic approach to managing sensitive information so that it remains secure. As defined in the ISO standards, it provides a model for; establishing, implementing, operating, and monitoring-reviewing, maintaining and improving of protection of information assets. [3]

Information Security is achieved through; implementation of applicable set of controls together with selected and adapted risk management process. IS is to be managed using ISMS model and IS controls need to be integrated with business processes of the organization. ISMS covers set of;

- Policies
- Processes
- Procedures
- Organizational structures
- SW and HW to protect the identified information assets

It is important to target manageable security, since it is not possible to achieve % 100 securities. The circular representation of information security management related concepts is given in Figure-1. Information is faced with; technology, human and environmental factors and related threats. Security circle is required to protect information via establishment of related standards, policies, processes and trainings. This various aspects need to be well managed with a systematic approach targeting manageable level of security.

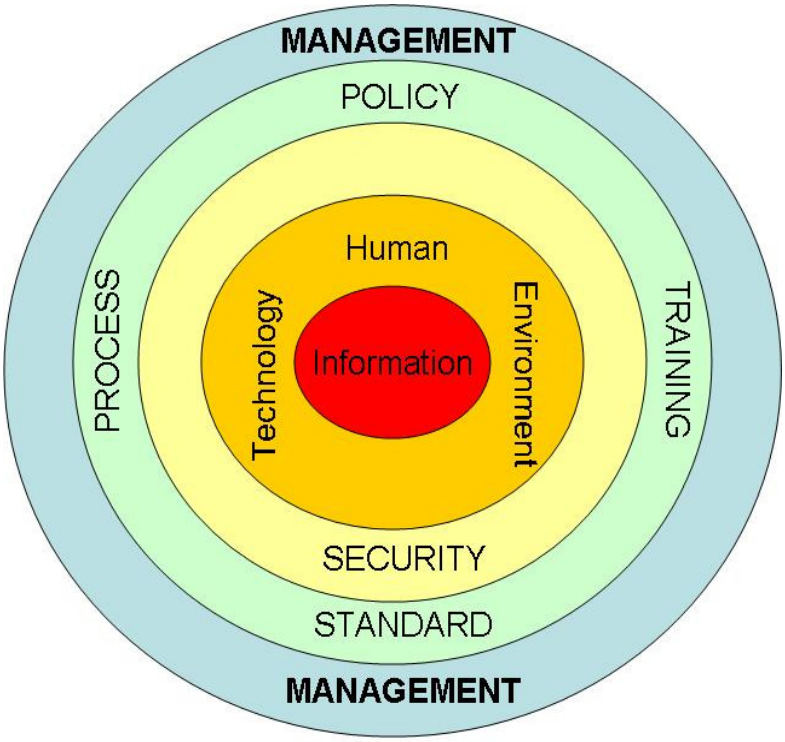


Figure 1. IS Related Concepts

2.4. STANDARDS FOR INFORMATION SECURITY MANAGEMENT

2.4.1. Overview of Information Security Standards

Awareness among the organizations is limited concerning the information security related topics; concepts, risks, legal basis, protection of information assets and security controls, international models and standards, good practices and implementations. No matter the initiating reason for an organization, international standards provide good practices and guidance for establishment of information security management systems (ISMS). They can be taken as basis and tailored to the specific security and compliance needs of the organization.

There are internationally accepted good practices and models that can be taken as guidance to establish and implement ISMS. Some widely known models are as follows:

i. International Organization for Standardization (ISO) Standards
ii. Control Objectives for Information and related Technology (COBIT)
iii. Information Technology Infrastructure Library (ITIL):

The effective use of best practices can help avoid re-inventing wheels, optimize the use of IT resources and even simple awareness and controls can reduce the occurrence of major IT risks.

ISO Standards

The International Organization for Standardization (ISO) is a non-governmental international body that collaborates with the International Electrotechnical Commission (IEC) in the development of international standards through technical committees. In the field of information ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

It is stated in ISO/IEC 27000:2012(E) that ISMS family of standards is intended to assist organizations of all types and sizes to implement and operate ISMS. ISO 27000 families of standards provide best practice guidance and recommendations on ISMS, in fact to any organization that handles and depends on information. The key standards within the ISO family of standards that are closely related with ISMS and 27001 are defined below. [3]

ISO/IEC 27000: *Information security management systems — Overview and vocabulary:* provides fundamentals and vocabulary for the ISMS standards.

ISO/IEC 27001: *Information security management systems — Requirements:* ISMS requirements standard, a specification for ISMS. It is the certification standard against which organizations' ISMS may be certified.

ISO/IEC 27002: *Code of practice for information security management.* It provides set of information security control objectives and a set of generally accepted good practice security controls. This can be used hand in hand with the Annex-A (controls) of the 27001 standard.

ISO/IEC 27003: *Information security management system implementation guidance.* Implementation guide for ISMS

ISO/IEC 27004: *Information security management — Measurement.* IS measurement standard suggesting metrics to help improve the effectiveness of ISMS.

ISO/IEC 27005: *Information security risk management.* ISO standard methodology for risk management. It can be used as guidance for building the risk management methodology as part of establishment of ISMS.

ISO/IEC 27006: *Requirements for bodies providing audit and certification of information security management systems.* Accreditation standards and a guide to the certification / registration process. Organizations providing certification has to be compliant with this standard.

ISO/IEC 27007: *Guidelines for information security management systems auditing.* Provides guideline for auditing information security management systems. [3]

27000 is a family of standards which also include other guidelines for specific sectors such as telecommunications, financial services. ISO/IEC 20000 is international standard providing guidelines for service management system. It specifies requirements for the service provider who wants to take it as reference for building and maintaining ISMS. [6]

This study focuses on the ISO/IEC 27002:2005 and ISO/IEC 27001:2005 which form the common basis and practical guideline on information security.

COBIT

COBIT provides a maturity model for IT Governance and controls. COBIT Security Baseline focuses on the specific risks around IT security in a way that is simple to follow and implement for small and large organizations. COBIT helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. The framework addresses both business and IT functional areas across an enterprise and considers the IT-related interests of internal and external stakeholders. provides globally accepted principles,

practices, analytical tools and models to help increase the trust in, and value from, information systems. Enterprises of all sizes, whether commercial, not-for- profit or in the public sector, can benefit from COBIT. [7]

ITIL

The Information Technology Infrastructure Library (ITIL) is a collection of best practices in IT service management (ITSM), focusing on the service processes of IT. It provides a practical framework for identifying, planning, delivering and supporting IT services to the business. It was developed by the United Kingdom's Office of Government Commerce. ITIL is typically used in conjunction with other good practices to manage information technology such as COBIT, ISO 27000. It describes processes, functions and structures that support most areas of IT Service Management and one of the many processes it describes is Information Security Management. Framework covered by ITIL has relevance to the ISO/IEC 20000. [8]

2.4.2. ISO/IEC 27001 ISMS Requirements

ISO/IEC 27001 can be considered as an overall framework that combines the management of; risk, security, governance and compliance. It helps the organizations in ensuring the harmonization of people, processes and technologies correctly in place. Organization can become aware and get prepared proactively in advance for managing security and risk. Since information asset is widely created-processed-stored in digital environment and organizations are becoming more dependant on information-critical processes, the ISO/IEC 27001 standard becomes more valuable. [9]

ISO/IEC 27001:2005 is a reference model and internationally accepted specification and certification standard for establishing ISMS. It can be used as basis to establish security framework. It is flexible and can be tailored according to specific requirements of the organization. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets.

ISO 27001 standard is comprised of 8 topics and annexes as listed in Table 1.

Table 1. Topics of 27001 Standards [2], [10]

Introduction	Explaining the process approach PDCA used by the standard
1. Scope	Specifying generic requirements of ISMS
2. Normative references	ISO/IEC 27002:2005 is considered essential to be used
3. Terms and Definitions	Briefly defining formalized glossary
4 ISMS	Content of the basis of the standard based on PDCA cycle • General requirements • Establishing and managing the ISMS (establish, implement and operate, monitor and review, maintain and improve) • Documentation requirements
5 Management Responsibility	• Management commitment • Resource management
6. Internal ISMS Audits	• Periodic internal audits • Defining opportunities for improvement and need for changes
7. Management Review of the ISMS	• Review suitability, adequacy and effectiveness of the ISMS • Review input, output
8. ISMS Improvement	• Continual improvement • Corrective action • Preventive action
Annex-A : Control Objectives and Controls	• List and description of the control objectives and controls (should be used together with ISO/IEC 27002
Annex-B: OECD Principles	(informative) Shows the relevance of the standard with 7 key principles laid out in the OECD Guidelines for the Security of Information Systems and Networks
Annex-C: Correspondence between standards	(informative) Correspondence of the standard with • ISO 9001:2000: Quality management systems - requirements • ISO14001:2004: Environmental management standards

For the purpose of 27001 compliance, chapters 4 to 8 (inclusive) must be covered. Annex-A covers the controls to be taken as reference for the establishment and implementation of ISMS and it is a summary of the controls from ISO/IEC 27002.

Process approach can be defined as the application of a system of processes within an organization, together with the definition and interactions of these processes and their management.

The process approach for the ISMS presented in the ISMS family of standards is based on the operating principle adopted in ISO's management system standards commonly known as the Plan – Do – Check – Act (**PDCA**) process. [2]

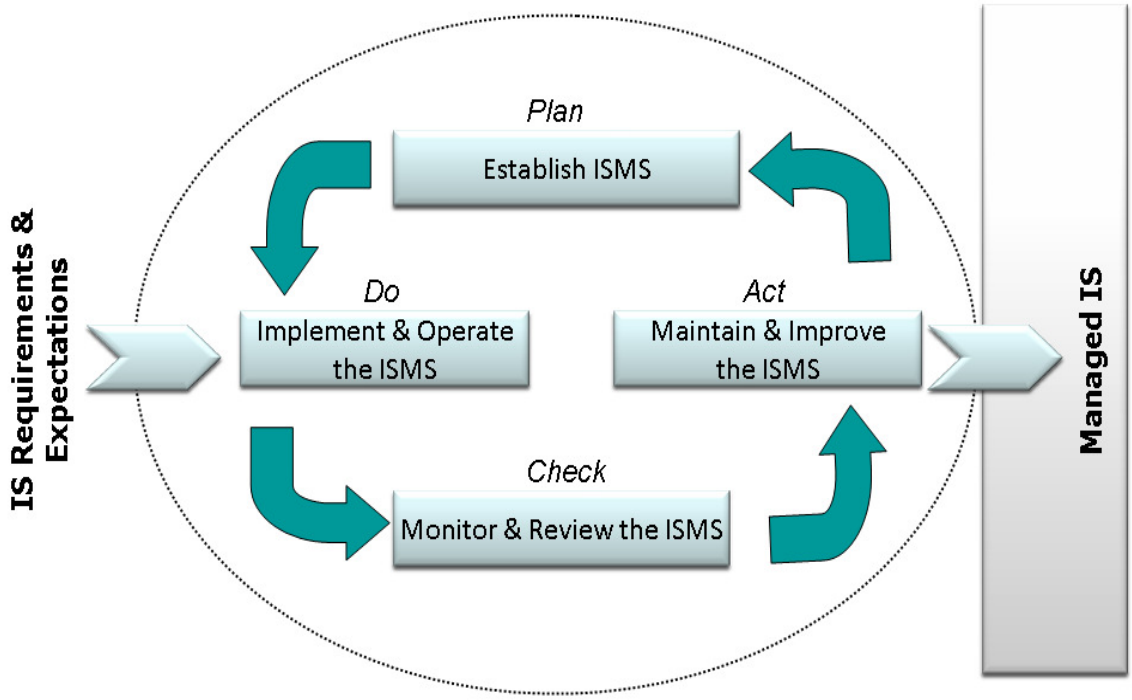


Figure 2. PDCA Model Applied to ISMS Processes [2]

a. **Plan** (establish the ISMS): At this phase, organization taking ISO as reference can decide-plan and establish own ISMS policy, objectives, processes and procedures based on own IS requirements and in line with the organization's overall policies and objectives.

b. **Do** (implement and operate the ISMS): At this phase, organization can execute the plan and put into operation the prepared ISMS policy, controls, processes and procedures.

c. **Check** (monitor and review the ISMS): This phase has importance to check and confirm that the implemented ISMS is running as planned. The organization can review and assess as relevant, measuring the actual performance against the set policy and objectives. The results in practice are then reported for management review.

d. **Act** (maintain and improve the ISMS): This phase covers the actions taken to fix the identified issues during the previous phase. It consists of taking corrective and preventive actions according to the internal assessment results and management review to enable persistent improvement of the ISMS. [2]

The process approach can be referenced during establishing-implementing-monitoring-maintaining-improving the ISMS. The same approach can also be used for the processes within the organization supporting the ISMS.

The overview of history of evolvement of the ISO/IEC 27001 standards briefly is as follows.

1992: The Department of Trade and Industry (DTI), part of the UK Government, published a 'Code of Practice for Information Security Management'.

1995: This document is amended and re-published by the British Standards Institute (BSI) in 1995 as BS7799. BS7799 was conceived, would enable an organization's management to assure itself that its information security measures and arrangements were effective. BS7799 focused on protecting the availability, confidentiality and integrity of organizational information and these remain, today, the driving objectives of the standard. BS7799 was originally just a single standard and had the status of a “Code of Practice”. In other words, it provided guidance for organizations. It was not a specification that could form the basis of an external third party verification and certification scheme.

1999: The first major revision of BS7799 was published. This included many major enhancements. Accreditation and certification schemes were launched and BSI was the first certification body.

2000: In December, BS7799 is again re-published, this time as a fast tracked ISO standard. It became ISO 17799 (or more formally, ISO/IEC 17799).

2002: A second part to the standard is published: BS7799-2. This is an Information Security Management Specification, rather than a code of practice. It begins the process of alignment with other management standards such as ISO 9000.

2005: A new version of ISO 17799 is published. This includes two new sections, and closer alignment with BS7799-2 processes.

2006: ISO 27001 is published, replacing BS7799-2, which is withdrawn. It is revised version of the British Standard's BS 7799-2. This is a specification for an ISMS, which aligns with ISO 17799 and is compatible with ISO 9001 and ISO 14001.

2007: ISO published technical corrigendum and replaced "17799" of the original ISO/IEC 17799:2005 standard with the new number 27002. Thus, name of the code of practice was brought into line with the 27000 family of standards. [9], [10], [11], [12]

2.4.3. ISO/IEC 27002:2005

ISO/IEC 27002:2005, the current issued version of "Information technology - Security techniques - Code of practice for information security management" is an internationally-accepted standard of good practice. It provides practical guideline for organizations in building their information security management standards and practices.

ISO/IEC 27001; formally defines the mandatory requirements for an ISMS and it uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS. 27002 is merely a code of practice-advisory document, rather than a formal specification and certification standards such as ISO/IEC 27001, that outlines what it is necessary to do in order to meet the 27001 specification and it guides by using the wording of "should" and "may". Organizations are free to select and implement other controls depending on their own policy and decisions. ISO/IEC 27001 Annex A incorporates a summary of controls from ISO/IEC 27002. In practice, ISO/IEC 27001

is referenced together with ISO/IEC 27002 and organizations that adopt the former also substantially adopt the latter. [13]

The standard outlines a set of controls in each area of ISMS and then gives implementation guidance on the way the control objectives can be met. It lays out a structured set of controls to address information security risks, covering confidentiality, integrity and availability aspects. The intention is that these suggested controls are selected and applied against risks identified through a risk assessment. It consists of 11 main clauses covering the following areas.

1. **Security Policy** Provides management direction and support for IS (i.e. IS policy document; preparation, approval, publish, dissemination, review)
2. **Organization of Information Security** - governance and management of IS within the organization as well as with external parties, in order to maintain the security of the organization's information. (i.e. assignment of IS responsibilities, confidentiality agreements, security in 3rd party agreements)
3. **Asset Management** - Inventory and classification of information assets, to effectively establish and maintain their protection. (i.e. asset inventory and classification, asset ownership)
4. **Human Resource Security** - Security aspects for employees joining, moving and leaving, for contractors and third party users to understand their responsibilities and to reduce the risk of misuse of facilities. (i.e. roles and responsibilities, IS awareness, removal of access rights)
5. **Physical & Environmental Security** - Provides controls to protect against unauthorized physical access or damage to the organization, computer facilities and information assets. (i.e. physical entry controls, equipment security both on and off premises, equipment maintenance)
6. **Communications and Operations Management** – Management of technical security controls to ensure secure and correct operation of

information processing facilities both within the organization and with third party interactions (i.e. document management, change management, malicious code controls, back-up, network security, electronic messaging, logging, monitoring of 3rd party service delivery).

7. **Access Control** - Restriction of access rights to networks, systems, applications, functions and data (i.e. user access management, password management, unattended user equipment, network access, application access)
8. **Information Systems Acquisition, Development and Maintenance** - Building security into applications (i.e. requirement analysis, input/output data validation, cryptographic controls-key management, development process).
9. **IS Incident Management** - Anticipating and responding appropriately to security breaches (i.e. reporting of IS events, weaknesses).
10. **Business Continuity Management** - Protecting, maintaining and recovering business-critical processes and systems. (i.e. continuity plans including IS, risk assessment).
11. **Compliance** - Ensuring conformance with information security policies, standards, laws and regulations (i.e. intellectual property rights, compliance with security policies and standards, regulation of cryptographic controls, information system audit) [1]

Under the 11 main clauses there are total of 39 control objectives and total of 133 controls in the standard. The relevance between the clauses and their relevant control objectives and controls is shown in Table 2.

Table 2. ISO/IEC 27002 Clauses-Control Objectives-Controls [2]

27002 Main Control Clause	Control Objectives	Controls
Security Policy	• Information security policy	2
Organization of Information Security	• Internal organization • External parties	11
Asset Management	• Responsibility for assets • Information classification	5
Human Resources Security	• Prior to employment • During employment • Termination of change of employment	9
Physical & Environmental Security	• Secure areas • Equipment security	13
Communications & Operations Management	• Operational procedures and responsibilities • Third party service delivery management • System planning and acceptance • Protection against malicious and mobile code • Back-up • Network security management • Media Handling • Exchange of information • Electronic commerce services • Monitoring	32
Access Control	• Business requirements for access control • User access management • User responsibilities • Network access control • Operating system access control • Application and information access control • Mobile computing and teleworking	25
Information Systems Acquisition, Development and Maintenance	• Security requirements of information systems • Correct processing in applications • Cryptographic controls • Security of system files • Security in development and support processes • Technical vulnerability management	16
IS Incident Management	• Reporting IS events and weaknesses • Management of IS incidents and improvements	5
Business Continuity Management	• IS aspects of business continuity management	5
Compliance	• Compliance with legal requirements • Compliance with security policies and standards, and technical compliance • Information systems audit considerations	10
Total of 11 control clauses	Total of 39 control objectives	133 controls

The mind map in Figure 3 summarizes and outlines the main sections of the standard.

Figure 3. Summarized Outline of ISO 27002 [13]

The numbering in the above outline start from four since the earlier sections covers introductory information and definitions.

Among the control clauses policy should be owned by the management with direct involvement and the least direct involvement of management can be said to be on clause 11, 12 and 13. This has been illustrated in Figure 4. [12]

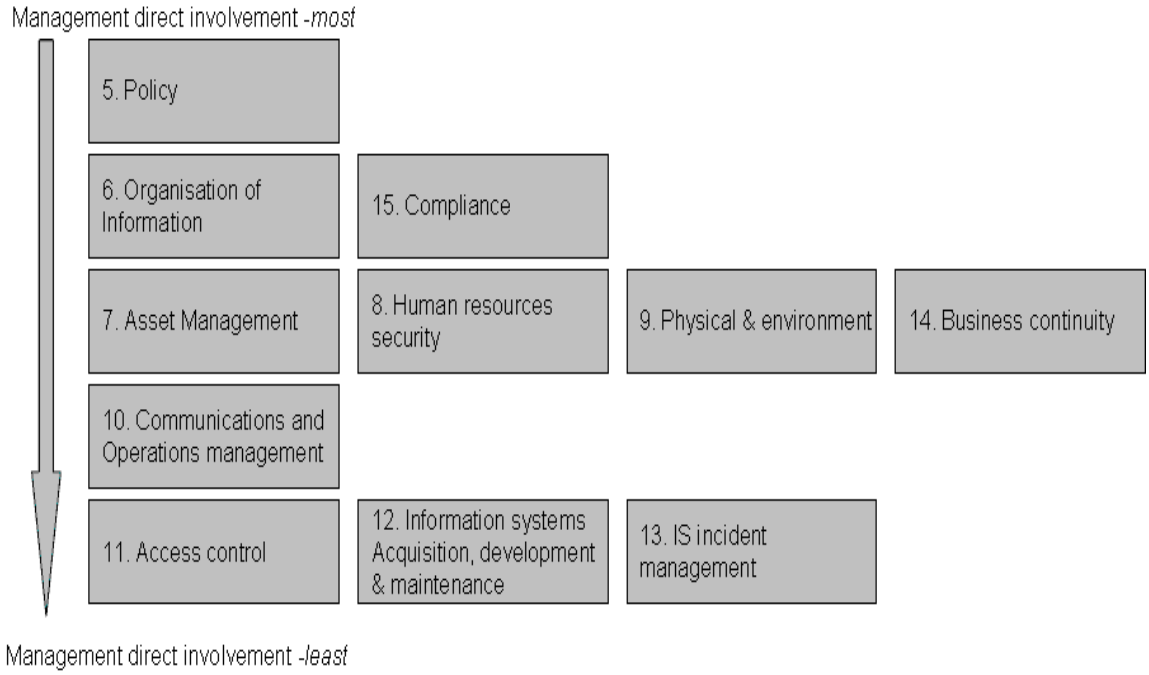


Figure 4. Management Involvement to the Implementation [13]

Organizations that adopt ISO/IEC 27002 must assess their own information security risks and apply suitable controls, using the standard for guidance. The control objectives make a very good starting point. None of the controls are mandatory and it is up to the users to select and implement controls that suit them, using a risk-assessment process to identify the most appropriate controls for their specific requirements. Other controls which are not listed in the standard can also be conducted provided that the organization's control objectives are satisfied. But if the organization wants to be compliant to ISO/IEC 27001 due to any reason (legal compliance, certification) and if organization decides not to adopt something (i.e. antivirus controls), this decision should be made knowingly and with proper justification as result of risk management decision process. [13]

2.5. IMPLEMENTATION STEPS AND ADAPTING TO ISMS

It is evident that adopting ISMS can help the organization in developing countermeasures to IS-related vulnerabilities. [9]

Most activities in IS management can be linked to three fundamental questions and answering them can lead to their respective result.

1. What needs to be protected: Identification of assets
2. Against what does it have to be protected: Identification of threats
3. How can it be protected: Identification and selection of proper countermeasures [25]

According to author's experience in information security related projects and consulting services; ISMS implementation steps start with organization's awareness and management ownership. Its design and implementation depends on the organization's;

- Needs and objectives
- Security requirements
- Business processes employed
- Size and structure of the organization
- Reflect requirements of all stakeholders

Successful implementation of ISMS depends on;

- Awareness and commitment of the management
- Definition of correct focus and objectives
- Commitment of the assigned key staff
- Doing what is written and writing what is being applied
- Commitment for maintaining

Phases of execution for ISMS implementation can be grouped as follows.

1. Preparation phase:
    a. Awareness assessment and understanding overall status
    b. ISMS Team assignment and their training
    c. Defining IS Scope and boundaries of ISMS
    d. Awareness Raising in organization

2. Implementation phase:
    a. Defining corporate IS policy
    b. Defining information assets
    c. Risk analysis-evaluation-management plan
    d. Selection of Controls (27001 Annex A)
    e. Statement of Applicability (SoA)
    f. Preparation of: policies-procedures-standards-instructions
    g. Management review and approval
    h. Training and awareness (continual)
    i. Execute: Operation and Records

3. Monitoring and Improvement phase:
    a. Overall implementation review and assessment
    b. Detailed assessment and internal audit
    c. Reviews, monitoring for improvement
    d. Continual awareness raising programs at all levels
    e. Taking corrective and preventive actions

Initiating the awareness of self status and understanding of requirements are important key milestone for organizations who work with information assets nevertheless are not quite aware information security aspects and do not know where to initiate. Organizations that are already quite aware due to reason such as legal compliance or business nature can also make use of self assessing their current status. Regular review and monitoring even after the ISMS is in place is also necessary for continuous improvement. Taking these into account, this thesis focuses to support mainly 1.a and 3.a. in the above list of items but can also support items; 1.d, 1.g and 3.d. For organizations who are not obliged to be certified should still take these steps to ensure their business continuity. Certification should not be the objective, but with proper adaptation of ISMS, certification can be an evident milestone.

The officially announced number of 27001 certification by country as April 2013 is provided in Table 3.

Table 3. Number of ISO/IEC 27001 Certificates per Country as of April 25th 2013 [14]

Japan	4152	Netherlands	24	Belgium	3
UK	573	Saudi Arabia	24	Gibraltar	3
India	546	UAE	19	Lithuania	3
Taiwan	461	Bulgaria	18	Macau	3
China	393	Iran	18	Albania	3
Germany	228	Portugal	18	Bosnia Herzegovina	2
Czech Republic	112	Argentina	17	Cyprus	2
Korea	107	Philippines	16	Ecuador	2
USA	105	Indonesia	15	Jersey	2
Italy	82	Pakistan	15	Kazakhstan	2
Spain	72	Colombia	14	Luxembourg	2
Hungary	71	Russian Federation	14	Macedonia	2
Malaysia	66	Vietnam	14	Malta	2
Poland	61	Iceland	13	Mauritius	2
Thailand	59	Kuwait	11	Ukraine	2
Greece	50	Canada	10	Armenia	1
Ireland	48	Norway	10	Bangladesh	1
Austria	42	Sweden	10	Belarus	1
Turkey	35	Switzerland	9	Bolivia	1
Turkey	35	Bahrain	8	Denmark	1
France	34	Peru	7	Estonia	1
Hong Kong	32	Chile	5	Kyrgyzstan	1
Australia	30	Egypt	5	Lebanon	1
Singapore	29	Oman	5	Moldova	1
Croatia	27	Qatar	5	New Zealand	1
Slovenia	26	Sri Lanka	5	Sudan	1
Mexico	25	South Africa	5	Uruguay	1
Slovakia	25	Dominican Republic	4	Yemen	1
Brazil	24	Morocco	4	**Total**	**7940**

The actual number of organizations having certification can be higher than what is showed in this table since some organizations may not want to be disclosed in the report. But the table clearly demonstrates that the total number officially disclosed is substantially high in Japan compared to even the next follower.

2.6. IS AWARENESS AND IMPLEMENTATION ASSESSMENT

Information security awareness concept is developing a culture of security within an organization and not just training or education.

The information security awareness is the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities and acts accordingly. Information security awareness is a dynamic process, made even more difficult with the continuously changing risks. Awareness and training programs lead from “become aware” to “stay aware” and end up in “be aware”, which changes security culture definitively. [4]

An organization can utilize a method, model or tool to assess the information security awareness level as well as implementation level. Basing the assessment to the international standards and best practices is the most appropriate approach. If organization has to comply due to regulatory obligation then the specific requirements or standards can be taken as basis of assessment.

Initial assessment can be done as starting point when the organization wants to understand its own awareness or status on information security. It can be in form of checklist or questions. More detailed questions can be used to assess when the organization wants to comply with a specific standard such as ISO-/IEC 27001 which has detailed controls. Similar approach can be used when organization has established information security management system and wants to measure its implementation level to monitor or improve.

The model or tools relevant to the assessment of IS implementation have been identified and reviewed during the literature survey.

2.6.1. Assessment Model of Information Security Implementation Levels

According to the study below [5]; in spite of all the efforts, security threats continue to occur with the main reason of organizations not being aware of the IS levels that they are practicing. It proposes a measurement model for assessing IS implementation levels in organizations and consists of three maturity levels that determine the degree of IS addressed. The model has been developed with the intention to be used by organizations to determine their levels of maturity in information security, in order to define what needs to be improved.

The model takes into account the three maturity models in security as listed below and their respective measurement levels:

i. Maturity levels in Systems Engineering Capability Maturity Model (SE-CMM)
ii. Maturity levels in Control Objectives for Information Related Technology (COBIT)
iii. Maturity levels in National Institute of Standards and Technology (NIST)

Each have different focus; SE-CMM model focuses on safety of the design engineering software, COBIT model focuses on specific audit procedures whereas NIST model focuses on documentation. But all three commonly have 5 maturity levels.

Based on the standards and other relevant studies, the model classifies 4 factors associated with information security and their respective measurement parameters that are demonstrated in Figure 5.

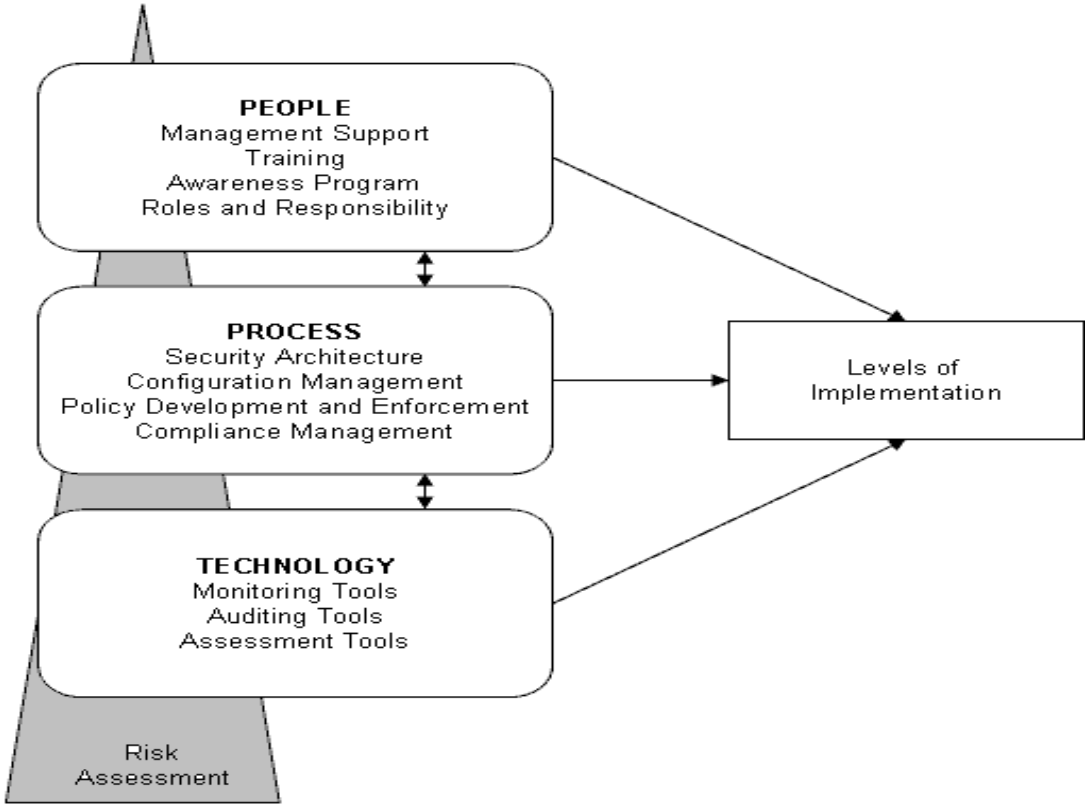


Figure 5. Assessment Model of IS Implementation Levels [5]

The model implies that the management should ensure that the people are aware of their roles and responsibilities by assigning as well as organizing necessary awareness and training programs. The remaining processes can be defined provided that the people aspect is correctly in place. Technology supports the processes. And the risk assessment should be present at all levels. The model categorizes the IS implementation maturity to 3 levels and to measure IS implementation it defines dimensions to the parameters based on the degree of importance of each parameter. It is shown in Table 4.

Table 4. IS Implementation Maturity Levels [5]

Level	Factor	Dimension
Level1: Basic	People Process/Procedure Technology Risk Assessment	Low Low/Non-existence Non-existence Low
Level2: Intermediate	People Process/Procedure Technology Risk Assessment	Moderate Moderate Low/Moderate Moderate
Level3: Advanced	People Process/Procedure Technology Risk Assessment	High High High High

Low: 0-25%; Moderate 25-75%; High >75%

Basic level is where aspects are partially addressed and management support might be inadequate. Awareness may be low; roles-responsibilities may not be properly set and understood. Process/procedures may be either not set or at minimal whereas technology is not used. In intermediate level the status is better but needs improvement. Advanced level all aspects are assumed to be addressed adequately. Thus, this model can be used by organization as a checklist for self-assessment during internal review.

2.6.2. Information Security Measures Benchmark (ISM Benchmark)

In order to support the organizations in Japan in building and improving their information security measures, Information-technology Promotion Agency (IPA) of

Japan has developed and released an assessment tool named ISM-Benchmark. According to IPA, numbers of users who have used this self-assessment tool have largely increased since it was first released in 2005. The number of users is over 13,000. The intention was to contribute in increasing the information security level of Japanese enterprises and it is evident that it is continuing to serve its purpose. [23]

Number of ISO/IEC 27001 Certificates per Country given in the Table 3 clearly shows that Japan has 4152 recorded companies having international ISO IS certification. This number clearly supports that the organizations in Japan have benefited this tool.

The tool facilitates questions that are prepared taking into account ISO information security standards and enables organizations to check the level of their security measures. The tool is available both in Japanese and in English. It also facilitates benchmarking to the user to compare their scores with the scores in the database established with recent 2 years of collected data from Japanese organizations.
This comparative and quantitative web based tool provides questions derived from security measures in ISO information security standards and include managerial, personnel, technical and physical controls. It covers 2 parts; one with questions concerning IS countermeasures and the other with questions about corporate profile. Organizations are classified into groups based on their information security risk index indicating risks to which organization is being exposed. Risk Index is calculated based on; the number of employees, sales figures, the number of critical information held, etc. The tool provides assessment results in numbers and charts such as scatter chart, radar chart and frequency distribution chart. [23]

During the course of this thesis study, it was interesting to identify this tool having similar objective and target users and that it has achieved in serving the community with the wide user base. It has been a motivating factor as well as supportive justification of this study.

2.6.3. Information Security Survey 2013 Benchmark

PricewaterhouseCoopers (PwC) has published a tool in their web site in which an organization can benchmark its own security profile against its peers compared with the data based on the Global State of Information Security Survey 2013 results conducted by PwC in conjunction with CIO and CSO magazines. [24] More detailed information concerning the survey method is provided in section 2.7.2. This web based benchmarking tool provides 6 steps as explained below;

Step1: Welcome - Getting started: In this step some information about the organization is requested; organization's annual revenue, primary industry sector, region of employment. Annual revenue can be selected as one of the following; Small, Medium, Large or Non-profit/Government/Education. The primary industry sector can be selected among the seventeen in the given list such as; Aerospace & Defense, Consulting/Professional Services, Consumer Products and Retail, Education /Non-profit, Engineering / Construction, Financial Services, Government Services, Health Industries, Technology, Telecommunications, Transportation and Logistics, etc.. The region can be selected from one of the following; North America, South America, Asia, Europe, Middle East and South Africa.

Step 2: Security spending: In this step, there are 3 questions. One is selection of business issues or factors that drive the organization's IS spending with selection items such as; company reputation, compliance, business continuity, hactivism, etc. Other questions are related to total IS security budget of the organization and if it increased/decreased/remained the same compared to previous year.

Step 3: Policies, strategies and safeguards: Includes questions with checkbox selections in order to assess the IS preparedness of the organization with policies, strategies and safeguards such as; issues included in the organization's security policy, IS and data privacy safeguards that are in place, initiatives that the organization launched to address mobile security risks.

Step-4: Security incidents: This step includes questions related to incident management such as; the estimated source of security incidents (current

employees, former employees, customers, hactivists, etc.), number of security incidents in one year period, if the organization has contingency plan in place to manage and report such incidents.

Step 5: Efficacy of security activities: This step contains questions related with the efficacy of managing IS activities such as; if the security policies align with company business objectives, self evaluating how well the IS is managed and the awareness at employee level.

Step 6: See how you compare: At this step personalized benchmark report is prepared and it can be viewed as well as downloaded in pdf format.

This is a useful tool which contains to the point questions to get view and approaches of the organization related to IS. Providing the results in to the user together in comparison with up-to-date survey data within the same industry, similar size scale and in the same region can provide useful benchmarking and reference point to the organizations.

2.6.4. Awareness and Implementation Level Assessment: Case in Turkey

The ISO/IEC 27001 has been accepted by TSE as Turkish standard for Information technology – security techniques – ISMS- Requirements as TS ISO/IEC 27001 with publication date 2.3.2006. The ISO/IEC 17799 (27002) has been accepted by TSE as Turkish standard for Information technology – security techniques – Code of practice for ISM as TS ISO/IEC 17799 with publication date 21.12.2006. [15]

TS ISO/IEC 27001 is in Turkish including the guideline of controls in Annex A. TS ISO/IEC 17799 is not in Turkish. It has valuable supplementing details for the implementation of the ISMS.

There are only two tools identified that are implemented and commercially available in Turkey which organizations can use throughout the lifecycle of ISMS implementation. One is ISMart, Information Security Management Software developed by BizNet for organizations that need to establish and maintain an ISMS

according to ISO27001 standard. Organization can categorize and define assets, conduct risk analysis and management for assets, select controls among ISO 27001 as well as create custom controls, produce reports, management of documents related with ISMS process, manage security incidents. Questionnaires can be used for measure effectiveness of ISMS, for understanding awareness level and gaps to fulfill for compliance requirements of the standard. [16] Another tool which is newly launched is Invento PRO product developed by Invento and with the Turkish user interface it is intended to provide supportive framework for compliance with information security standards and regulations such as ISO 27001, COBIT, etc. [17]

When organization decides to establish and maintain its ISMS in compliance with international security standards, such tools can be procured by the organization to provide structured guidance. Organization can also prefer to follow the guidelines of the standards and built their own approach without utilization of such tools.

There is also on-line training content in Turkish regarding information security awareness including topics such as; what is information security, computer and access security, threats and methods for protection, internet and network security. It has been prepared by The Scientific and Technological Research Council of Turkey, Informatics and Information Security Research Center (TÜBİTAK BİLGEM) Cyber Security Institute under “Information Security E-Learning Project” and it can provide a good source for basic awareness content for individuals and organizations. [18]

Due to regulatory compliance; organizations in the financial sector and telecommunication sector are well aware and ahead of the other sectors in IS implementation. Others, especially the SMEs should raise their awareness and strengthen their institutional capacity on IS aspects and management.

There is no overall awareness and implementation assessment tool in Turkish that is available in a web site where organizations, which may or may not have prior knowledge of information security aspects, can perform self-assessment as well as benchmark their status with organizations having similar IS risk level.

2.7. CASE REVIEWS

2.7.1. Information Security and Cybercrime Survey

According to the first annual Irish Information Security and Cybercrime Survey conducted by Deloitte in association with EMC in May 2012 [19], the average cost per organization for a security incident over one year is €41,875. The survey includes Irish information security leaders of multinationals, Irish organizations and subsidiaries. The sectors covered include; financial services (27%), IT (hardware/software) (15%) and government (17%) percent. Other sectors are with smaller percentage and include; Education, Telecom/ISP, Manufacturing, Semi-state, Pharmaceuticals, Transport and Insurance.

The survey showed that within one year period, unprecedented number of high profile information security incidents, data breaches, cyber attacks, and instances of cybercrime both nationally in Ireland and globally. Irish organizations have never faced such a myriad of advanced technological threats and attacks on their digital and critical assets.

Based on the survey the following include the resulting key observations:

50% of respondents believe that employees and their activities presented the biggest challenges in information security. This is followed by technical threats and attacks with 29%. This result shows that human factor is very important aspect in information security and employee knowledge of information security and procedures is not sufficient causing security risks.

44 % of respondents stated that they believe board members have an average understanding of information security risks. This shows the lack of management awareness which leads to lack of ownership. General business alignment on information security and related activities is not well integrated with business risks.
68% of respondents stated that no action was taken following an investigation of internal or external incidents. This shows the lack of established and ongoing ISMS

and incident management. Most organizations are reactive in the event of a security or cybercrime incident, and deal with incidents as they happen.

Regulatory and legislative compliance is the lead motivating drivers for security activities, investment and adopting information security management system and technologies with 45%. This shows that the organizations are concerned with regulatory compliance rather than cyber threats or incident management. Top security initiative of organizations is information security training and awareness with 23% followed by other technical ones such as data protection and technology investment.

Main reason for information security investment is to satisfy the regulatory requirements with 33% which is more than protection of brand reputation and minimizing damages and losses with 28% each.

While 54% of the organizations had not experienced any security breaches in the past 12 months, 32% identified between one to five security breaches. Among the security attacks/breaches; hacking had the highest portion with 38%, followed by privilege misuse as 21%. This is complimented with view of 23% of incidents identified involved internal personnel as either the cause/suspect for cybercrime. Other security breaches included; physical attack and malware as 13% each followed by social engineering as %8.

Large majority (70%) of the information security professionals surveyed believed that their organization was on par with, if not better their peers.

There is no database or tool that is used to assess their status in comparison to their peers in the country.

2.7.2. Global State of Information Security Survey 2013

The Global State of Information Security Survey 2013 has been conducted by PricewaterhouseCoopers (PwC) in conjunction with CIO magazine and CSO magazine. It has been conducted online and worldwide between February and April

2012. Organizations that are clients of PwC and readers of the two magazines were invited to take the survey. Result of the survey is based on the responses of over 9,300 high level managers such as; chief executive officers chief information officers, chief security officers, chief information security officers, vice presidents and directors of IT and IS from 128 countries. Among the collected information; forty percent of respondents were from North America, 26% from Europe, 18% from Asia, 14% from South America, and 2% from the Middle East and South Africa. The survey results as figures and graphics have also been used as source in the benchmarking tool explained in section 2.6.3. [24]

The survey results are published in PwC website. The user can select one of the listed questions to explore the collected data and view the results of the survey in graphic representation as well as drill down for different industries and regions. [20]

Based on the PwC the Global State of Information Security Survey 2013 some key results can be summarized as following; [20]

- The main estimated source of security incidents are current employees followed by former employees and then hacktivists.
- They believe that their employees considering all levels are not very aware but somewhat aware about cyber risks,
- Organizations are not very confident but somewhat confident that effective IS behaviors have been instilled into the organizational culture,
- They mainly use malicious code detection tools as technology safeguard, malware and virus protection software as data privacy safeguards,
- IS safeguards related to people are mainly; conducting personnel background checks and having people dedicated to employee awareness programs
- The driving force for IS spending is mainly economic conditions
- Mobile device security is mainly used to address mobile security risks,
- Main process IS safeguard in place is having overall IS strategy,
- Security strategy is in place mainly for employee use of personal devices on the enterprise and on mobile devices,
- Most of the organizations detected 1-9 security incidents in past 12 months,
- Organizations tend to increase their security spending.

2.7.3. Factors Influencing ISM in SMEs: Case Study from Turkey

The results of the study, which examines the enterprise information security in small and medium-sized enterprises (SMEs) in one of the big cities in Turkey in the year 2009 [21], shows that Turkish companies do not attach as much importance to information technology security as similar companies from different countries do. The results of the study were based on a survey questionnaire with 9 sections and total of 49 questions raised to 97 SMEs in the same city. When the 9 sections are reviewed, it can be seen that the sections take main clauses of ISO/IEC 27001 Annex A as reference only with slight differences.

i. Security Policy
ii. Organizational Security
iii. Asset Classification and Control
iv. Personnel Security
v. Physical and Environmental Security
vi. Communications and Operations Management
vii. Access Control
viii. System Development and Maintenance
ix. Business Continuity Management

The questions under the above sections are answered in 1 to 5 scales. (1: strongly disagree, 2: disagree, 3: undecided, 4: agree, 5: strongly agree)

The summary of the results of the study is as follows:

1. Most companies are not sufficiently aware and involved in IS standards to be able to implement in their organizations;
2. %50 of the companies faced security vulnerabilities in last 12-18 months;
3. The most common vulnerability is human carelessness, thus human factor being the weakest link in information security.

The study underlines that the current level of management awareness of these SMEs are not in sufficient level and suggests to formalize their IS policy by adapting a security standard.

CHAPTER III

APPROACH AND SCOPE

3.1. PURPOSE AND SCOPE OF IS AWARENESS AND IMPLEMENTATION LEVEL ASSESSMENT

In the number of companies per country as per official certification listed at ISO official web site, the disclosed number of organizations from Turkey is 35. [14]

The main target should be to improve information security implementation level even if certification is not targeted. But yet, increase in awareness can have positive impact to the increase in number of organizations having certification.

According to Prolexic Quarterly Global Distributed Denial of Service (DDos) Attack Report, Turkey is one of the top ten source countries for attack traffic in the second quarter of 2012 after China (33.79%), Thailand(23.63%), USA (8.76%), Indonesia (8.67%) which is (6.59%) for Turkey. Turkey was newly inserted to the list since it was not in the top ten list in the two previous quarter reports. [22]

According to the Information Policy Country Report on Turkey dated June 2009, Turkey is a relative latecomer to the development of laws on personal data security and privacy. According to the report, improvements will be beneficial in the aspects of data security and information processing security both for the public and private sector. The goal of the development of information security policies is to make private and government sector services more efficient, which includes some level of data security. The goal for Turkish security policy should be to strike an appropriate balance between information security and efficiency of economy. Since Turkey's particular geographic region and is important which is attractive for cyber attacks. [26]

Although information security policy and legal obligations as well as organizations having IS compliance have evolved since the time of publication of this report, increase in awareness and improvement in implementation is still necessary especially among SMEs, according to the results of recent case study from Turkey on factors influencing ISM in SMEs. [21]

The two focused standards 27001 and 27002 have been translated into Turkish and can be obtained from the Turkish Standards Institute (TSE). If the company wants to have more accessible environment to understand and assess its status, a simpler and overall guidance can be more beneficial both for initial awareness and monitoring the evolvement at later stage. Benchmarking with companies having similar security requirements can also have comparable and motivating effect for the organizations.

There is no web site in Turkish which can be used for self assessment of the overall organization that is based on international standards and at the same time provides some implementation tips as well as comparable benchmark. This thesis and the tool focus on the factors of IS; people and process/procedure, technology and risk assessment but at the same time focusing on prototyping a web based self assessment environment basing the assessment questions on the widely known and accepted ISO standards for information security.

Prototype model and tool has been designed and implemented based on the ISO security standards and composed of eight main sections and their relevant assessment questions and guidance tips. The eight sections are shown in Figure 6.

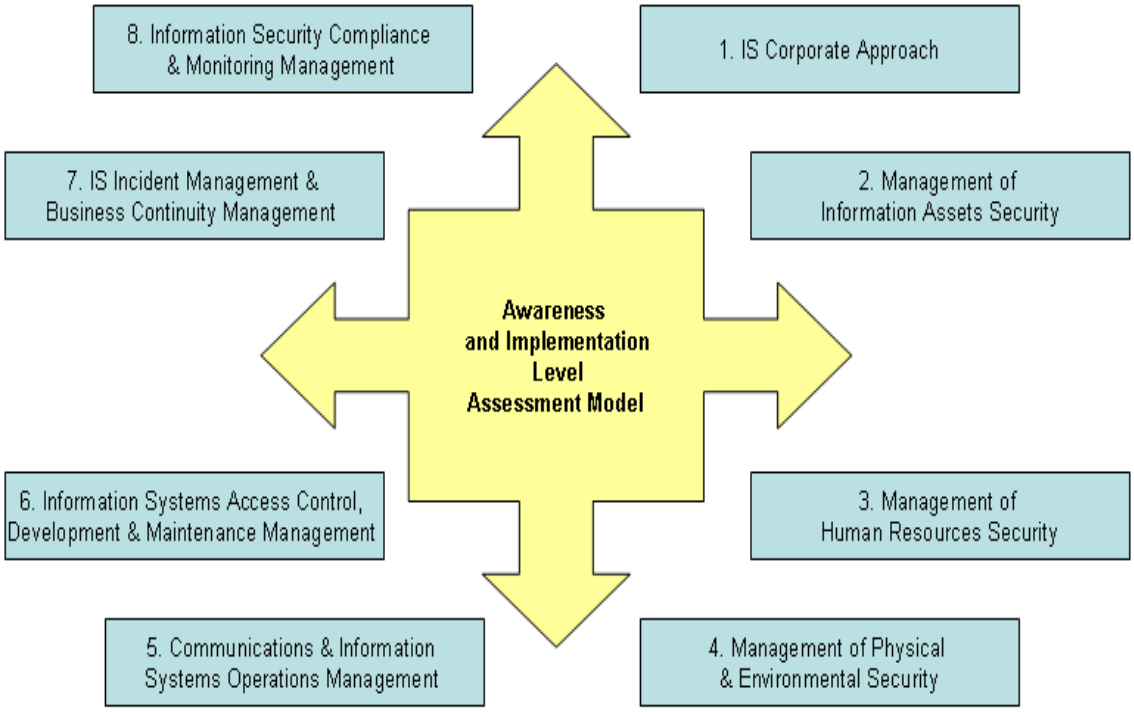


Figure 6. Assessment Model Components

3.2. ASSUMPTIONS AND DEPENDENCIES

The model and the prototype tool is targeted to serve for general overall assessment and targets all levels of users who may not have prior sufficient level of understanding or training on information security. The questions are targeted to be limited in total, short and understandable by wide variety of user levels including management level. Some useful tips have also been provided to more clarify the content of the question.

The model contains data for benchmarking. This data has been established by taking expert views from experts who have long-term experience on information security domain and consulting-auditing based on ISO family of standards to wide sector coverage in Turkey. Due to the sensitivity and nature of the subject of information security, organizations are hesitant to provide their level of information security for benchmarking, thus this approach was more objective and accessible for

this study. The benchmark values in the model are based on mean values of 3 experts reflect approximate values as ideal and average based on expert views.

3.3. ASSESSMENT MODEL BASED ON SECURITY STANDARDS

The questions of the assessment have been prepared based on ISO/IEC 27002 control objectives. During the preparation of the assessment questions the standards given in Table 5 have been elaborated, related to information security;

Table 5. Elaborated International IS Standards

ISO/IEC 27001:2005	Information technology – Security techniques – Information security management systems Requirements
ISO/IEC 27002: 2005	Information technology – Security techniques – Code of practice for information security management

Since the interface is prepared in Turkish the standards given in Table 6, which have been accepted as Turkish standard related to information security have been elaborated;

Table 6. Elaborated Turkish Standards on IS

TS ISO/IEC 27001 (March 2006)	Based on ISO/IEC 27001 (2005) Information technology – Security techniques – Information security management systems Requirements
TS SO/IEC 17799 (December 2006)	Based on ISO/IEC 17799 (2005) Information technology – Security techniques – Code of practice for information security management

ISO/IEC 27002 contains 11 security control clauses and each of the clauses contains main security categories which is 39 in total. In addition, there is also one introductory clause concerning risk assessment and treatment. In detail there is total of 133 controls under these set of control clauses. While logically grouping the questions, similar approach has been used and the set of control objectives of the standard has been taken into account.

The Table 7 shows the 27001 Annex A control clauses which are also the same as 27002 and the number of controls under the relevant control set. The table also shows the chapters of the assessment tool in comparison with the standard. In assessment tool, 8 sections have been identified which cover all 11 clauses of the standard. Some clauses with closer topics have been logically grouped. Three

questions have been prepared for each section in the assessment tool for even distribution in the assessment result.

Table 7. ISO/IEC 27001 Annex A and the Assessment Model

Assessment Model Sections	**# of Qs***	**Relevant ISO/IEC 27001:2005 Annex A. Control Clause (number of control objectives within the clause)**	**# of Cs****
Section 1 - Information Security - Corporate Approach	3	A.5*** Security Policy (1)	2
		A.6. Organization of Information Security (2)	11
Section 2 - Management of Information Assets Security	3	A.7 Asset Management (2)	5
Section 3 - Management of Human Resources Security	3	A.8 Human Resources Security (3)	9
Section 4 - Management of Physical & Environmental Security	3	A.9 Physical & Environmental Security (2)	13
Section 5 - Communications and Information Systems Operations Management	3	A.10 Communications & Operations Management (10)	32
Section 6 - Information Systems Access Control, Development and Maintenance Management	3	A.11 Access Control (7)	25
		A. 12 Information Systems Acquisition, Development and Maintenance (6)	16
Section 7 - IS Incident Management and Business Continuity Management	3	A. 13 IS Incident Management (2)	5
		A. 14 Business Continuity Management (1)	5
Section 8 - Information Security Compliance and Monitoring Management	3	A.15 Compliance(3)	10
Total 8 Chapters	Total: 24	Total of 11 control clauses	Total: 133

- ** Number of Questions, ** Number of Controls*
- ****numbering of the clauses in the standard start with 5 since 27002 has 1-4 sections with introductory information and 27001 Annex A is in compliance with this numbering.*

Assessment tool has total of 24 questions; 3 questions under each section with total of 8 sections. Some clauses which can be logically grouped have been grouped. 8 sections have been determined also considering the graphical presentation to be used in the assessment result.

According to the 27002 standards, a number of controls can be considered as a good starting point for implementing information security. They are either based on essential legislative requirements (depending on applicable and relevant legislation)

or considered to be common practice for information security. In the introductory section of the standard, there is a list of controls considered to be essential to an organization in two different aspects; legislative and common practice. These are given in Table 8 and how they are covered in the assessment tool.

Table 8. ISO/IEC 27002 Essential Controls and the Assessment Model

27002 Controls Essential in Legislative Aspect [1]	**Assessment Model Sections**	**Assessment Model Question**
Data protection and privacy of personal information	8. Information Security Compliance and Monitoring Management	Q 22, Q 23
Protection of organizational records		
Intellectual property rights		
27002 Controls Considered to be Common Practice for IS [1]	**Assessment Model Sections**	**Assessment Model Question**
Information security policy document	1. Information Security - Corporate Approach	Q 1
Allocation of information security responsibilities		Q 2
Information security awareness, education, and training	3. Management of Human Resources Security	Q 7
Correct processing in applications	6. Information Systems Access Control, Development and Maintenance Management	Q 18
Technical vulnerability management		
Business continuity management	7. IS Incident Management and Business Continuity Management	Q 20, Q 21
Management of information security incidents and improvements		Q 19

3.4. ASSESSMENT SECTIONS AND RELEVANT ITEMS

In the model, each of the 8 sections in the assessment consists of 3 questions related to the section. Each question is assigned a short descriptive title, in order to utilize in the resulting output of the assessment. The Table 9 shows each section and short descriptive title of 24 questions.

Table 9. Assessment Model Sections and Question Titles

Assessment Tool Sections	Descriptive Title of Each Question
1. Corporate Approach to Information Security	1. Information Security Policy
	2. IS Management Organization
	3. Corporate Staff and Third Party Contracts-Agreements
2. Management of Information Assets, Risk Assessment & Management	4. Protection of Information Assets
	5. Categorization/Classification of Information Assets
	6. Risk Assessment of Information Assets
3. Management of Human Resources Security	7. Information Security Awareness and Training
	8. Information Security Roles and Responsibilities
	9. Human Resources Security during Employment or Termination of Personnel
4. Management of Physical & Environmental Security	10. Physical Security
	11. External People/Parties Physical Security
	12. Equipment Security
5. Communications and Information Systems Operations Management	13. Operational Information System Security
	14. Protection Against Malicious Software
	15. Information Communication Facilities Security
6. Information Systems Access Control, Development and Maintenance Management	16. Information Systems and Data Access Security
	17. Network Access Security
	18. Information Systems Development and Maintenance
7. IS Incident Management and Business Continuity Management	19. Information Systems Security Incident Management
	20. Information Systems Possible Failure / Interruptions Handling
	21. Business Continuity Management
8. Information Security Compliance and Monitoring Management	22. Compliance with Legal Requirements Related to IS
	23. Compliance with Security Policies and Standards, Technical Compliance
	24. IS Management Monitoring and Audit
Total 8 Sections	*Total of 24 Questions*

3.5. MEASUREMENT SCALE IN THE ASSESSMENT MODEL

For answering the questions and scoring of the answers, 1 to 5 scaling has been used. The approach and description of the scaling is listed in Table 10.

Table 10. Assessment Model Measurement Scaling

Scale	Short Description	Description
1	Not being applied	The management is not aware of its necessity; awareness-raising at corporate level is required.
2	Awareness is in place but yet not applied	Management is aware of its necessity, planed to be applied; no policy or rule/control has been established.
3	Partially applied	Rules and controls are applied occasionally or at partial manner. Policy and rules are not or partly in written.
4	Applied but no periodic monitoring is being conducted	Rules and controls are applied organization wide and they are in written. But periodic monitoring-review is not being conducted.
5	Applied, monitored-audited and improved based on organization's changing requirements	Rules and controls are applied organization wide and they are in written. In addition; periodic monitoring-audit, review of results and necessary improvements are being conducted.

3.6. PREPARATION OF QUESTIONS IN THE ASSESSMENT MODEL

Considering all of the above steps and their outputs, the questions for the assessment model have been prepared. They are carefully prepared taking into account the control objectives in the standards but at the same time balancing the level of technical content with simplicity in order to target wide range of users at various levels of management and technical knowledge. The questions are targeted to be limited in number, short and understandable considering the targeted users.

The content of the control in the standards are covered in general but each control of the standard is not covered one to one. Content of the controls are sometimes merged or some more technical ones are left out. Questions statements are designed to be simple but they have detailed sub-questions under the main question text which enlarges the content of the question. This enables to cover the content of more than one control that be related to the same main question and merge them under one single question.

Under most of the questions useful notes and tips have been incorporated with the aim to further clarify the content of the question as well as to create more awareness and better understanding of the related IS topic.

In order to best serve the targeted users in Turkey, the questions are prepared in Turkish language.

The questions are given below including short descriptive titles and their relevant questions. The useful tips are provided only in the tool and in Turkish language.

1. Information Security Policy

Organization has corporate security policy and rules for IS.

- Information security policy document is prepared in written,
- The policy document is approved by the management, applied and reviewed-updated as necessary,
- It is communicated to all employees and relevant external parties.

2. IS Management Organization

Organizational structure has been established for IS management.

- Management takes ownership, actively supports and encourages IS,
- IS roles and responsibilities are clearly defined and assignments are done,
- A committee has been formed for IS activities with representatives from different departments/units of the organization,
- Following up-to date information on IS by regular follow-up of appropriate contacts such as national security forums and web site of relevant institutions.

3. Corporate Staff and Third Party Contracts-Agreements

Critical IS requirements have been addressed in contracts of employees and external parties and precautions are supported with legal basis.

- Confidentiality and nondisclosure agreements have been done with

employees and contractors including the IS aspects,

- Security requirements are covered in agreements and contracts with external parties having access to organization's information or information processing facilities. For example; external service providers, maintenance and support services for information systems, software development services, etc. (do not consider this bullet if outsourcing is not applicable)
- Security requirements are addressed and confirmed before giving access to customers to the organization's information or assets. (do not consider this bullet if no external access)
- Necessary measures are taken on legal basis to prevent information-data leakage, loss of data, miss-utilization of data or information system

4. Protection of Information Assets

Appropriate countermeasures are applied for protection of organizational information assets (including personnel and confidential data).

- Key organizational assets have been identified and inventory maintained,
- Ownership (person or department responsible for its protection) of information assets have been defined,
- Protection of information assets is applied throughout all the processes such as; acquiring, creating, using, maintaining, transmitting, deleting and disposal,
- Security countermeasures are in place for information assets processed in both manual or information processing facilities.

5. Categorization/Classification of Information Assets

Key organizational information assets are grouped and classified based on their level of importance to the organization and countermeasures-rules defined based on their criticality and managed accordingly.

- Key organizational assets have been grouped taking into account their value, legal requirements, sensitivity and criticality to the organization,
- Rules are defined and applied for managing according to their classification,
- The responsible people/units have been defined and assigned who are responsible in protection of relevant information assets,

- Labeling is done according to classification of information assets. In case application tool is being utilized same approach is applied

6. Risk Assessment of Information Assets

Risk evaluation and management is applied for the key information assets.

- Possible threat and vulnerabilities have been defined and evaluated,
- Security controls are established taking into account threats and vulnerabilities
- Corporate approach and method is defined and applied for risk management
- Periodic review is conducted on possible risks and countermeasures, updated as necessary,
- In case of presence of external parties accessing to organization information, relevant risks are identified, countermeasures are applied for protection of the relevant data and data processing facilities.

7. Information Security Awareness and Training

IS training program is conducted for all employees, awareness and training studies are performed periodically;

- Training program covers the management level and temporary personnel,
- Following the initial awareness raising, informative and training studies are organized periodically. The following are being covered; organization's IS policies and expectations, IS responsibilities, possible threats and vulnerabilities, precautions and rules, proper utilization of information systems facilities, (logon-access, password utilization, etc.),
- Training-workshop results and reflection to IS behavior are monitored.

8. Information Security Roles and Responsibilities

Employees (including temporary staff, contractors and third party users), before and during working with the organization and leaving, are been written informed on security-related roles and responsibilities, ownership has been obtained on relevant information security aspects.

- Employees are aware of their responsibilities and organization's IS requirements, provide advocacy and support for the implementation,

- Incentives are implemented for ownership of IS
- The disciplinary proceedings are in place in the event of a security breach detection.

9. Human Resources Security during Employment or Termination of Personnel

For all candidates for employment, contractors and third party users, background and reference checks are performed according to the relevant position. As employment contracts of the employees are terminated (including temporary staff, contractors and third party users), the processes are in place for returning of all organizational assets and removal of access rights to information and information processing facilities.

- Employees, temporary staff, contractors and third party users are aware of their responsibilities and organization's IS requirements during and termination of the employment.

10. Physical Security

The necessary security measures to prevent unauthorized physical access are being maintained in the institution building and parts that contain information and information processing facilities.

- Secure areas are being separated with door or wall from the external environment, and have access controls to allow access only to authorized personnel,
- All business areas and offices are protected against unauthorized physical access,
- The system room entrance is protected, and measures have been taken, allowing access to authorized personnel only,
- Physical protection is in place for secure areas, information and data processing environments and equipment against natural or man-made disasters.
- For the secure areas where sensitive data reside, validation of access is implemented as well as all access records (log information).

11. External People/Parties Physical Security

For the people entering and exiting the institution from outside the organization (customers, contracted third party company officials, cargo service, cleaning service, etc.), security related rules are defined and being implemented.

- Delivery operations are carried out in a separate area, outside the safe areas,

- A separate work area is reserved outside the safe areas of the institution, for the individuals and firms who are providing outsourced services,
- Guest acceptance is held in a separate area and outside the secure areas.

12. Equipment Security

The necessary measures have been taken to protect equipment, installations, and power and communication cables containing information assets or carrying data from natural or human-induced damage.

- Equipment is protected from unauthorized access and environmental threats, in order to reduce the risks resulting from hazards to ensure continuity,
- Necessary security policy is applied for the equipment which can be removed out of the institution (portable computers, storage devices, etc.). The data or software is securely deleted, in order to prevent unauthorized access to sensitive information within the equipment which will be reused or disposed.

13. Operational Information System Security

Necessary security measures are applied to protect the operational information systems and the related data.

- Information systems operating procedures are documented,
- To reduce the risk of unauthorized access; system development, testing and deployment system environment are separated. The rules are in place to prevent utilization of actual data in the test environment,
- Change management is held in the information systems. For example for major modifications; keeping track and log, planning and testing, defining possible security implications, rollback in case of problems,
- Data backup is done on a regular basis, tested and verified,
- Log records are kept for information systems utilization and security incidents and these logs are periodically reviewed,
- Duties and responsibilities are segregated to reduce opportunities for misuse.

14. Protection Against Malicious Software

Necessary security measures are taken and implemented against code of malicious software (computer viruses, worms, trojan horses, etc.) for the

protection of the information integrity.

- Protection software is used against malicious codes, prevention, detection and recovery controls are made,
- Necessary security patches are installed to prevent possible cyber attacks,
- Information system users are being informed for protection regarding malicious codes,
- Virus scans are performed for the mobile devices, which have been used outside of the institution, before connecting to the corporate network.

15. Information Communication Facilities Security

Necessary security measures are taken and implemented for the security of the information transferred using internal and external communication networks and systems.

- Encryption methods are used to protect the data subject to data transfer,
- Information in electronic messaging is protected,
- Online transactions are being protected from unauthorized alteration and data corruption of data integrity,
- The control measures are in place for the information being transmitted over the network used in-house and outside the boundaries of the institution,
- Measures have been taken against portable storage devices (USB memory stick, mobile computing, etc.) to protect against the risks of data loss or theft.

16. Information Systems and Data Access Security

Necessary countermeasures have been taken and implemented for the access to and authorized utilization of the data on the information systems

- The user identification, removal, access, password registration and management is made in systematic manner and periodically revised,
- The users are directed to follow good security practices regarding their password identification and use,
- Each user is given a separate unique user name and password which is the basis for access and authorization,
- The users are allowed and monitored access to information sources and

information system applications, according to their authorization levels and given privileges.

- Clean desk and clear screen policy adopted throughout the organization.

17. Network Access Security

The security measures applied for the network connection, within or outside access of the institution.

- Users can only have access to the services authorized for their use,
- Appropriate authentication methods are used to control remote access,
- If the organization has distributed offices and using wide area network connection, a separate logical network grouping made by taking into account the need for security. Different controls can be applied to groups,
- For the shared networks, especially beyond the premises of the organization, access is limited and in controlled way by taking into account the organization's remote access policy and business requirements.

18. Information Systems Development and Maintenance

The necessary security measures are applied during the development and maintenance of application software.

- For the institution specific application software (in-house developed or outsourced), security requirements and controls are determined and integrated during the requirements definition, design and development cycle,
- Necessary controls defined within the application software to avoid errors during data entry, preventing data loss or unauthorized modification or misuse, (data correctness-compliance, controls and possible measures to minimize the information disruption, and message integrity protection)
- Change management is made, and the major changes are tracked,
- The application software is tested for security weaknesses prior to deployment,
- The cryptographic methods are used to protect the completeness, integrity and confidentiality of the data,
- Regular monitoring and follow-up in order to prevent information leakage

(monitoring system and software are utilized for user and system activities, system resource usage)

- For the management of technical vulnerabilities, the potential vulnerabilities and appropriate measures are taken. (Keeping log-monitoring system, tracking software versions, where the software is installed- responsible person, tracking configuration changes, monitoring against possible attacks)

19. Information Systems Security Incident Management

Procedures for notification of security incidents or weaknesses are in place, in order to enable timely and corrective action.

- Methods are available to report the identified or suspected information security incidents,
- Information system users (all employees, contractors and third party users), have been briefed to report the security vulnerability or suspected cases,
- Methods are applied for effective, fast, responsive monitoring and evaluation against information security violation and information security incidents,
- In the event of a violation of the information security, communication channels to the external authorities (police, fire, telecommunication action service provider, equipment / services service provider, etc.) are defined.

20. Information Systems Possible Failure / Interruptions Handling

Necessary measures have been taken to ensure the availability of the established information systems in the event of malfunctions or interruptions,

- Necessary precautions are in place for system accessibility considering the necessary time to recover (i.e. backup system that can be deployed, tested-verified backups, keeping operational logs, etc.),
- Recovery steps and procedures of such interruptions are defied in written and the relevant staff is trained accordingly,
- In case of outsourcing, resolving of the system outage and accessibility issues are placed in the agreements.

21. Business Continuity Management

Business continuity management framework across the enterprise, plans and

systematic are established including aspects of information security.

- Events-possibilities-impacts that may cause interruptions for business continuity are determined,
- In the event of system failure, the affects (reflections to the critical business processes of the organization, important information assets, risks, and required time for the provision of the organization's business continuity) have been identified,
- IS requirements-precautions-necessary actions for business continuity are defined, responsibilities are set and relevant people and parties are informed, corporate staff has been trained,
- In case of outsourcing, the requirements are reflected to the business continuity agreements with service providers,
- Measures are taken to ensure the continuity in case of natural disasters.

22. Compliance with Legal Requirements Related to IS

All necessary measures are taken to avoid violations of law, legal, regulatory or contractual obligations in relevance with information security.

- All relevant regulatory and contractual requirements are defined by the organization, documented and kept up to date,
- The procedures are carried out according to intellectual property rights, the use of software products on the legal, regulatory and compliance requirements,
- Important corporate records are protected against delete, lost and counterfeiting,
- Confidentiality of personal information and data are protected,
- Monitoring is conducted and criminal and legal proceedings provided, to prevent unauthorized use and misuse of information processing facilities,
- Cryptographic controls are in compliance with legal regulations

23. Compliance with Security Policies and Standards, Technical Compliance

Management monitors and ensures the compliance to organization's security policies and standards.

- Managers ensure that security procedures in their areas of responsibility are properly carried out,
- Information system compatibility is within the set standards, hardware and software controls are implemented, and checked at regular intervals,
- Information security awareness level is reviewed; compliance with awareness-training program and awareness level is monitored.

24. IS Management Monitoring and Audit

Organization conducts internal audits; monitors the effectiveness of the procedures and controls and their compliance to the requirements.

- Internal audit activities are carried out at regular intervals in order for continuity of compliance,
- The compliance and effectiveness on the identified information security needs are reviewed,
- The audit and review studies are recorded, assessed and used for improvement.

3.7. GROUPING BASED ON LEVEL OF INFORMATION SECURITY REQUIREMENTS

To distinguish the organizations' requirements for security level, groups have been identified. The maturity levels in security standards and the reviewed IS assessment models during this study have been considered while deciding on the number of groups. To simplify but at the same time facilitate to distinguish the security needs, three groups have been identified and these groups are given in Table 11.

Table 11. Grouping Based on IS Risk Level in the Assessment Model

Group	IS Risk Level	Description
Group-1	**HIGH LEVEL** Information Security Measures are required	The organizations in this group host and/or service information of national/corporate secrecy or personal information that requires data privacy such as information of citizen. Such organizations have data security requirements and need high level information security countermeasures.
Group-2	**MEDIUM LEVEL** Information Security Measures are required	The organizations in this group host and/or service information that require certain level of security incorporating business confidentiality and/or personal information. Organizations in this group require lower level of data confidentiality than the group-1 thus requires medium level security countermeasures.
Group-3	**LOW LEVEL** Information Security Measures are required	The organizations in this group host and/or service information mainly not subject to data privacy and confidentiality. Compared to group 1 and group 2, lower level of information security countermeasures is sufficient.

The organization, based on its own IS risk level and security requirements, have to identify which group describe the status of the organization. The group that the organization best fits is to be selected by the organization.

3.8. DEFINITION OF FIELDS OF ACTIVITY

The provision of field of activity / sector information is optional information in the model. Referencing the official statistical program of Turkey 2012-2016 published by Turkish Statistical Institute, NACE codes have been used for the information technology utilization statistics. [27]

For the fields of activity / sector grouping in the model, Turkish Statistical Institute NACE Rev.2 Economic activity classification, 2013 has been referenced. Turkish of the NACE codes have been retrieved from the Turkish Statistical Institute web site and used in the assessment model and the tool. [28]

Statistical Classification of Economic Activities in the European Community Rev.2 abbreviated as NACE Rev.2 is internationally accepted coding standard, thus preferred and used for fields of activity-sector definition in the model. Originating authority of the NACE codes is the Commission of the European Communities (Statistical Office/Eurostat) [29]. Sector definition codes are listed in Table 12.

Table 12. Sector Definition in the Assessment Model

	NACE Rev.2
Code	**Definition**
A	AGRICULTURE, FORESTRY AND FISHING
B	MINING AND QUARRYING
C	MANUFACTURING
D	ELECTRICITY, GAS, STEAM AND AIR CONDITIONING SUPPLY
E	WATER SUPPLY; SEWERAGE, WASTE MANAGEMENT AND REMEDIATION ACTIVITIES
F	CONSTRUCTION
G	WHOLESALE AND RETAIL TRADE; REPAIR OF MOTOR VEHICLES AND MOTORCYCLES
H	TRANSPORTATION AND STORAGE
I	ACCOMMODATION AND FOOD SERVICE ACTIVITIES
J	INFORMATION AND COMMUNICATION
K	FINANCIAL AND INSURANCE ACTIVITIES
L	REAL ESTATE ACTIVITIES
M	PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES
N	ADMINISTRATIVE AND SUPPORT SERVICE ACTIVITIES
O	PUBLIC ADMINISTRATION AND DEFENCE; COMPULSORY SOCIAL SECURITY
P	EDUCATION
Q	HUMAN HEALTH AND SOCIAL WORK ACTIVITIES
R	ARTS, ENTERTAINMENT AND RECREATION
S	OTHER SERVICE ACTIVITIES
T	ACTIVITIES OF HOUSEHOLDS AS EMPLOYERS; U0NDIFFERENTIATED GOODS- AND SERVICES-PRODUCING ACTIVITIES OF HOUSEHOLDS
U	ACTIVITIES OF EXTRATERRITORIAL ORGANIZATIONS AND BODIES

3.9. EXPERT CONSULTATION AND ANALYSIS

After preparation of the questions, expert view has been received from the experts having extensive specific experience including ISO standards, information security as well as wide sector experience in Turkey. Some minor tunings have been made on the questions based on received comments.

In order to have benchmarking aspect in the model, each group needs to have ideal and average values that are pre-set in the database. For this purpose, consultation to the same experts has been received. A questionnaire form has been designed and prepared to be filled by the experts. The first introductory information page of the questionnaire is as follows.

A Prototype for Information Security Awareness and Implementation Level

This form is to take expert view. The approximate values will be calculated based on the expert views received regarding the ideal and average scores for each group.

While filling for the average, based on your experience, please consider the average level of the organizations belonging to the group. When filling for the ideal, based on your experience, please consider the status of the company/companies that you think/observe implement the information security measures in very good level.

Please provide your Expert View by filling the same form 2 times for each of the groups;

Identification of Average Level for Group-1
Identification of Ideal Level for Group-1
Identification of Average Level for Group-2
Identification of Ideal Level for Group-2
Identification of Average Level for Group-3
Identification of Ideal Level for Group-3

Selection of the Group based on the IS Risk Level:

Group-1: HIGH LEVEL Information Security Measures are required

Grup-2: MEDIUM LEVEL Information Security Measures are required

Group-3: LOW LEVEL Information Security Measures are required

Please select for which of the following the form is being filled

Use “X” to select	Filled for the following
	1. Identification of Avarage Level for Group
	2. Identification of Ideal Level for Group
	3. Identification of Avarage Level for Group
	4. Identification of Ideal Level for Group
	5. Identification of Avarage Level for Group
	6. Identification of Ideal Level for Group

Please indicate the sectors considered for the filling of the form

The remaining of the form consists of questions prepared for the model. It is specifically noted to the experts that the average value or the ideal value is not what the companies score “should be”. In defining the average score, the expert should take into account his/her experience sector and companies and consider and reflect the average level of the companies belonging to that group. In defining the ideal score, the expert should consider the companies that implement ISMS at very good level and reflect their status while answering to the questions.

Using this approach, ideal and average values for each group have been set. The benchmark values should be considered as approximate values based on the wide range of sector experience and specific domain and country experience of the experts. They are provided in 3 group basis not in the sector detail. Sector detail is only for informative purpose in the tool.

The results from the experts have been merged and mean average of the values of the experts have been used while constructing the average and ideal benchmark values in the database.

The resulting values from selected experts are given in APPENDIX A.

3.10. GRAPHICAL REPRESENTATION APPROACH

The assessment results can be best demonstrated if supplemented with graphical presentation. Thus, based on the relevant survey the radar chart is decided to be used for graphical method of displaying assessment data. It is in the form of a two-dimensional chart of three or more variables represented on axes starting from the same point. It is also commonly known as spider charts, web charts, or star plots. It is particularly useful when examining several factors that are related to one item which was the main reason for selection. [30]

CHAPTER IV

MODEL AND APPLICATION DEVELOPMENT

4.1. KEY FACTORS TO THE PROTOTYPE APPLICATION

The model built in the steps explained in the previous chapter has been implemented as a web based self-assessment tool. The key factors to the prototype application are:

i. It takes reference the internationally accepted IS standards ISO/IEC 27001:2005
ii. It is intended to be self explanatory-easy to use interface-accessible as web based application that is freely available for organizations' self assessment.
iii. It can be used to assess security measures at overall level with good balance of simplicity and technical information.
iv. It can be used to measure both awareness and implementation level for organization.
v. It can be used as tool to improve the understanding and ownership at management level.
vi. It can be used as benchmarking of the self status in comparison with organizations having similar level of security requirements.

4.2. DESIGN OF THE PROTOTYPE ISM ASSESSMENT TOOL

The tool has been implemented in three-tier architecture by using jsp/servlet technology. With three-tier architecture; presentation, application processing, and data management functions are logically separated.

Client Tier (Presentation tier): The web based user interface of the tool is the topmost level of the application which interacts with the user and user inputs and/or views information related to the services handled in the business tier.

For the assessment tool; client tier is a web browser. User can freely use among widely user browsers such as; Google Chrome, Mozilla Firefox or Internet Explorer.

Middle Tier (Application/Business Logic Tier): This tier is the gateway between the tool interface (presentation tier) and the database tier. It is where the application functionality is performed as the user inputs new or views the existing data from the database. For the assessment tool; the middle tier is implemented as J2EE Application Server.

Database Tier (Data/Persistence Tier): The data entered via the application interface and processed at application tier is stored into and retrieved from the database. The tier keeps data independent from the application servers or business logic and only deals with the queries.

For database, relational model has been used and PostgreSQL open source database has been used to implement the database. The database model of the prototype assessment tool is given in Figure 7:

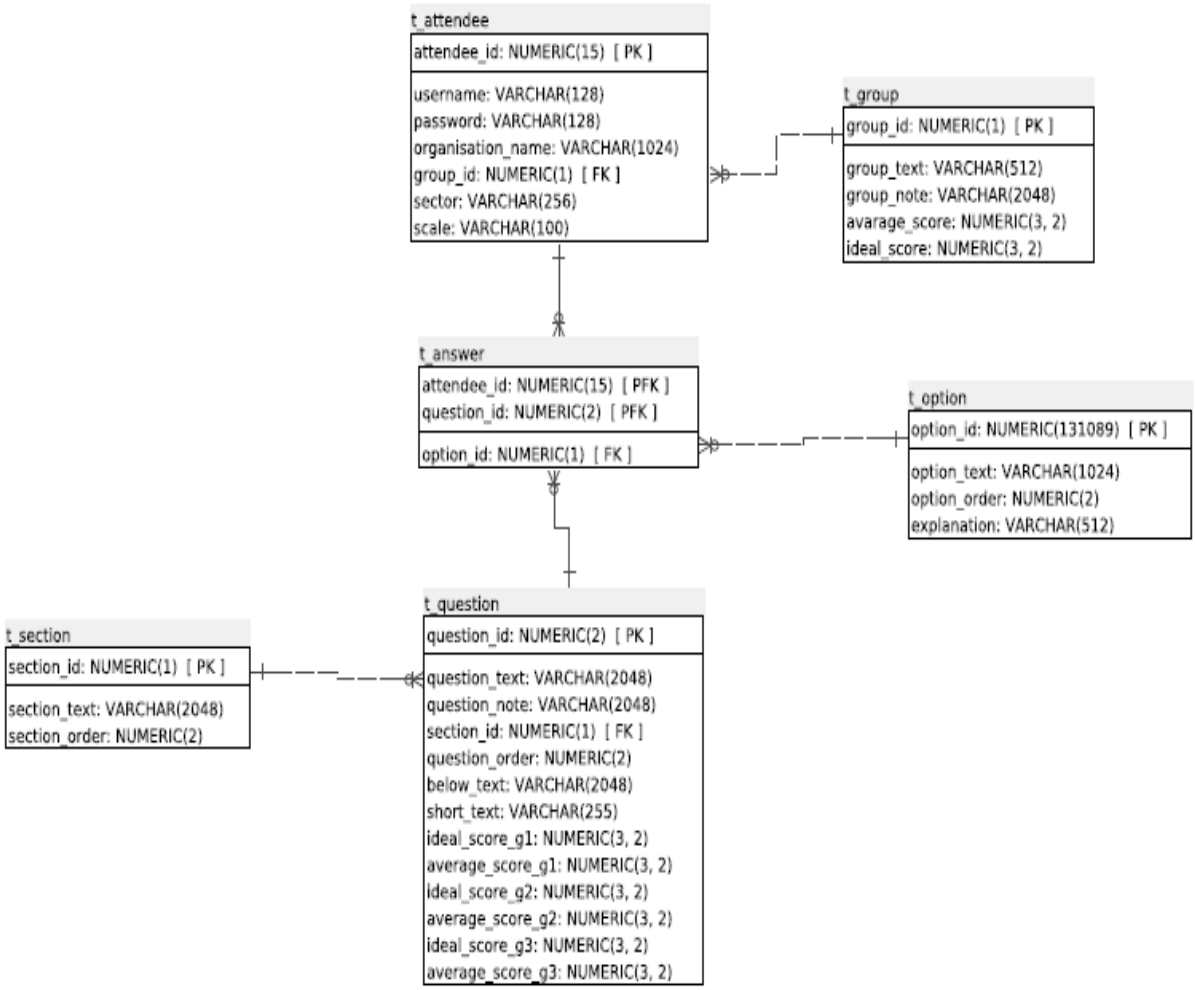


Figure 7. Data Model of the Assessment Tool

The entities and relationships between them can be seen from the above figure. Six tables are used to manage the data in the database.

4.3. IMPLEMENTATION OF THE PROTOTYPE ASSESSMENT TOOL

The tool has been implemented by using jsp/servlet technology and deployed on J2EE application server. Jsp/servlet technology is preferred to enable both platform and server independent flexible design and implementation. Code samples from the tool implementation are placed at APPENDIX B.

4.4. PROTOTYPE ASSESSMENT TOOL MODULES

4.4.1. Accessing the Tool

For the period of duration of the study, the application is placed on a server and made accessible via the given link.

http://www.kmo.com.tr/news1.asp?iKodHaber=106

The identified test users have used this link to access and use the tool.

4.4.2. Objective and Utilization Module

When the link is accessed the “objective and utilization” tab and its content is the default interface to the user.

Figure 8. Objective-Utilization Module

There is a user name and password fields in the top right corner.
For first time user, no user name is to be provided by the user in this tab. If it is first time user prefers to save his/her assessment to re-access in the future then he needs to provide user name password not at this stage but after the assessment is completed as shown Figure 9. User name-password is provided and save “Sakla” button is used to save the assessment record in the database with the relevant user name. Saving the results of the assessment for future re-access is optional.

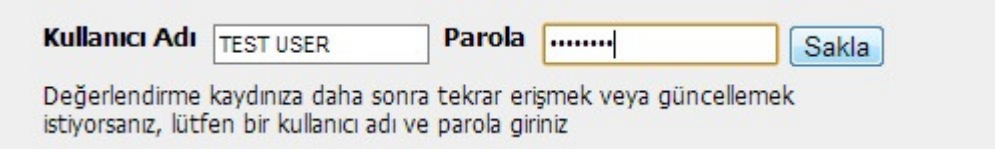


Figure 9. Saving for Future Re-Accessing to Assessment

If the user has previously conducted assessment and saved it by giving a user name-password then previous assessment record can be re-accessed. This can be done by providing the pre-defined username and password in this tab and using the entrance button “Giris” as shown in Figure 10. In this case, the user can modify if there is any status change in the assessment questions which will be reflected to the result of the assessment.

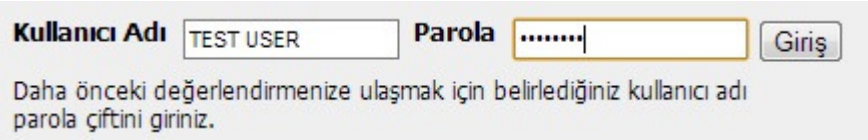


Figure 10. Re-Accessing the Previously Recorded Assessment

4.4.3. Organization Information Module

The second tab is used to access the “organization information” module interface. This page can be seen in Figure 11.

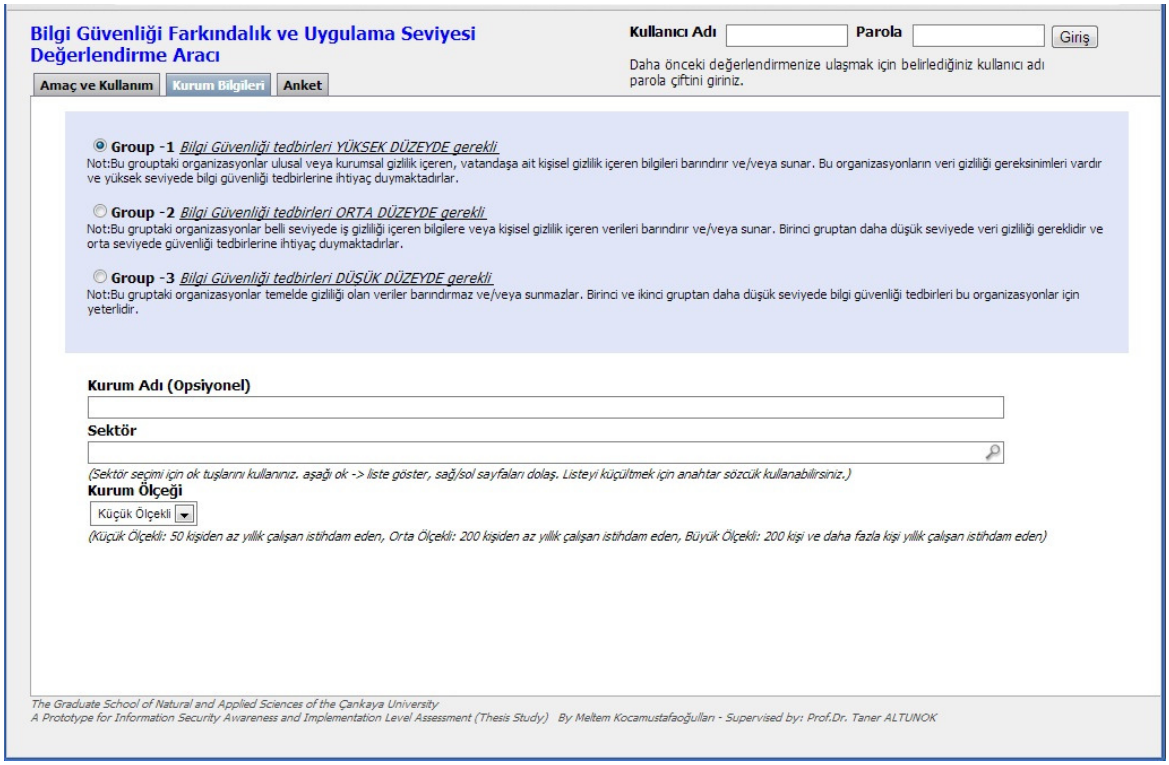


Figure 11. Organization Information Module

Based on the information security risk level and information security level requirement, organization should select one of the groups; Group-1, Group-2 or Group-3 of which the details are explained in Chapter 3. This information is required. The organization name (“Kurum Adı”) and sector information (“Sektor”) are optional and can be left blank. Organization name can be entered if the user wants to save or print the result having this information. If not it can be left blank or any other explanatory-reminder text can be placed if preferred. Sector information provides list of values by using down-up arrow to select and right-left arrows to move between its pages. The sector codes are the list of NACE Rev.2 codes as explained in Chapter 3.

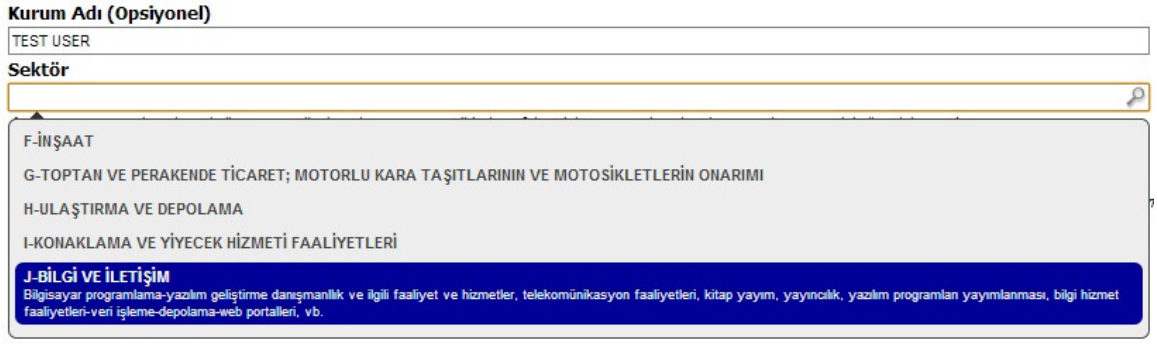
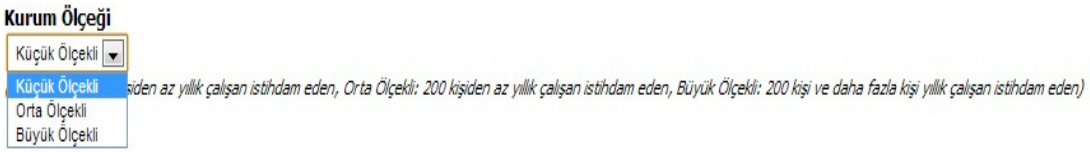


Figure 12. Selection of Sector Information (optional)

The size of the organization can be selected among the pre-defined list of values are as follows. If not selected the default value will be small size.

i. Small size (“Kucuk Olcekli”): Number of people < 50
ii. Medium size (“Orta Olcekli”): Number of people < 200
iii. Large size (“Büyük Olcekli”: Number of people >= 200



Selecting the sector code or size has no affect to the evaluation algorithm of the assessment.

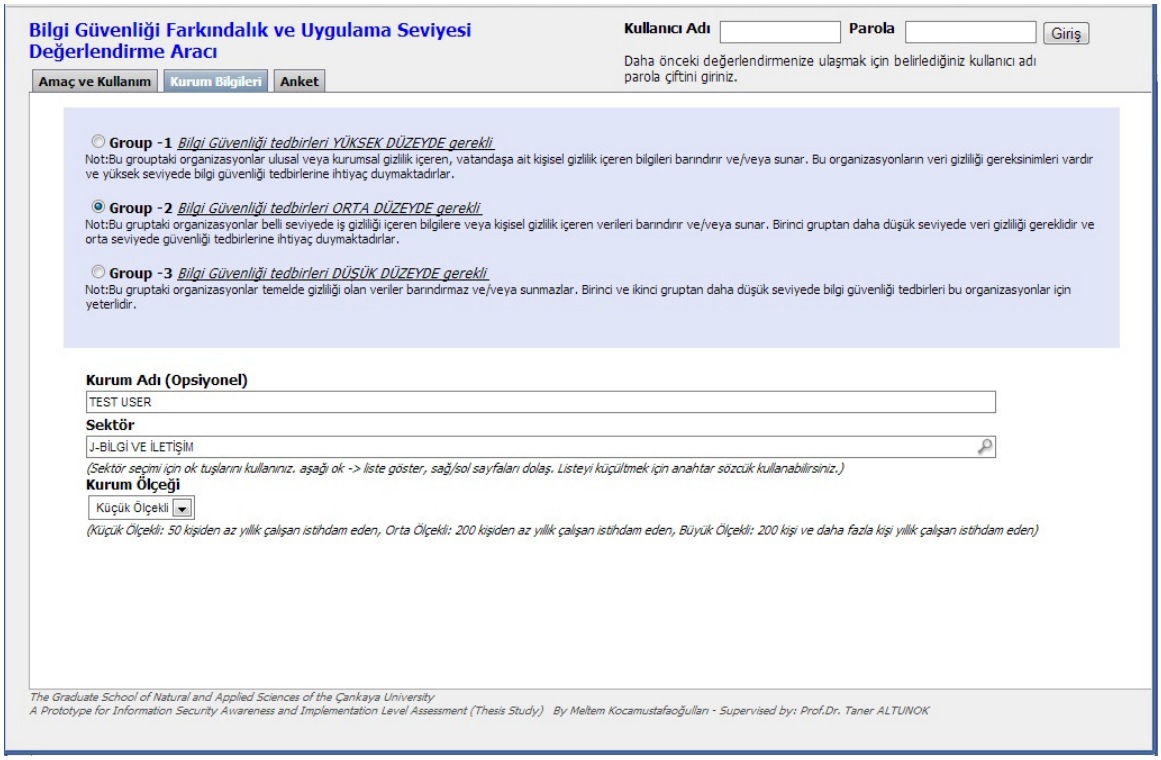


Figure 13. Organization Information Module with Sample User

4.4.4. Assessment Questions Module

The third tab is used to access the “Assessment questions” module interface. Here the first time user should answer all the questions in order to have proper assessment result. If the user is accessing previously saved assessment record, then modification is possible in the answers which will be reflected to the result. When all the questions are answered at the bottom right of the screen, there is button to complete (“Tamamla”). Review is recommended before the assessment is completed.

Assessment Questions Module has 8 sections having 3 questions per each section as defined in chapter 3. Some sample screens are given in Figure 14, Figure 15, Figure 16, Figure 17, Figure 18, Figure 19, Figure 20 and Figure21.

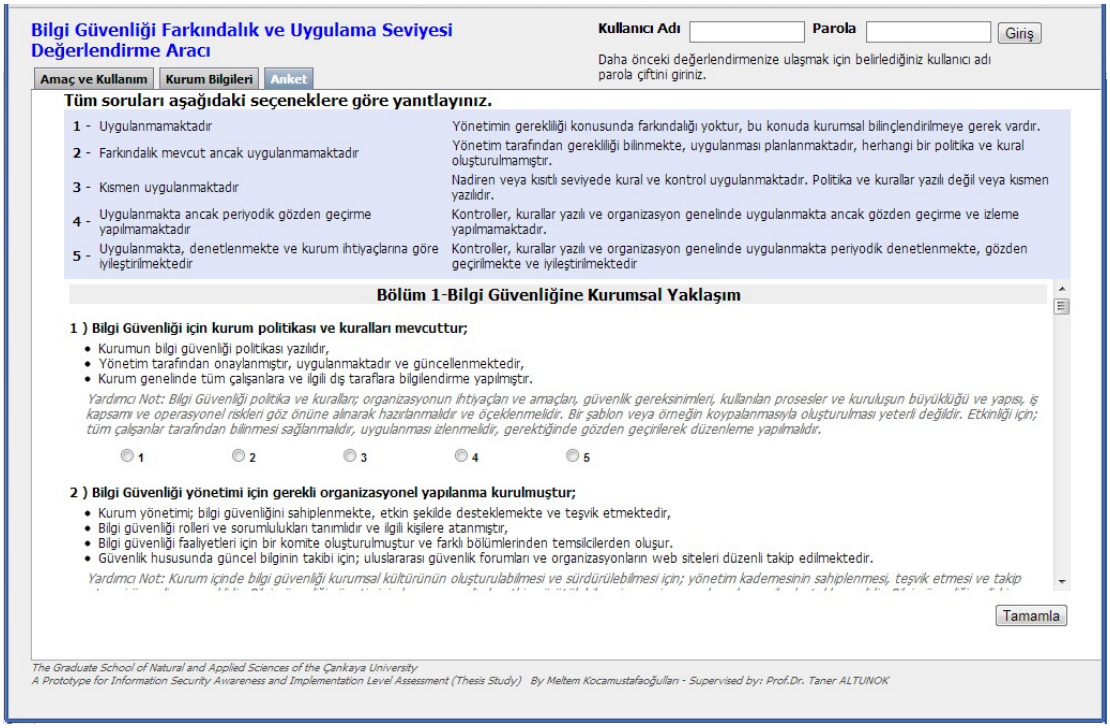


Figure 14. Assessment Questions Module-Section 1

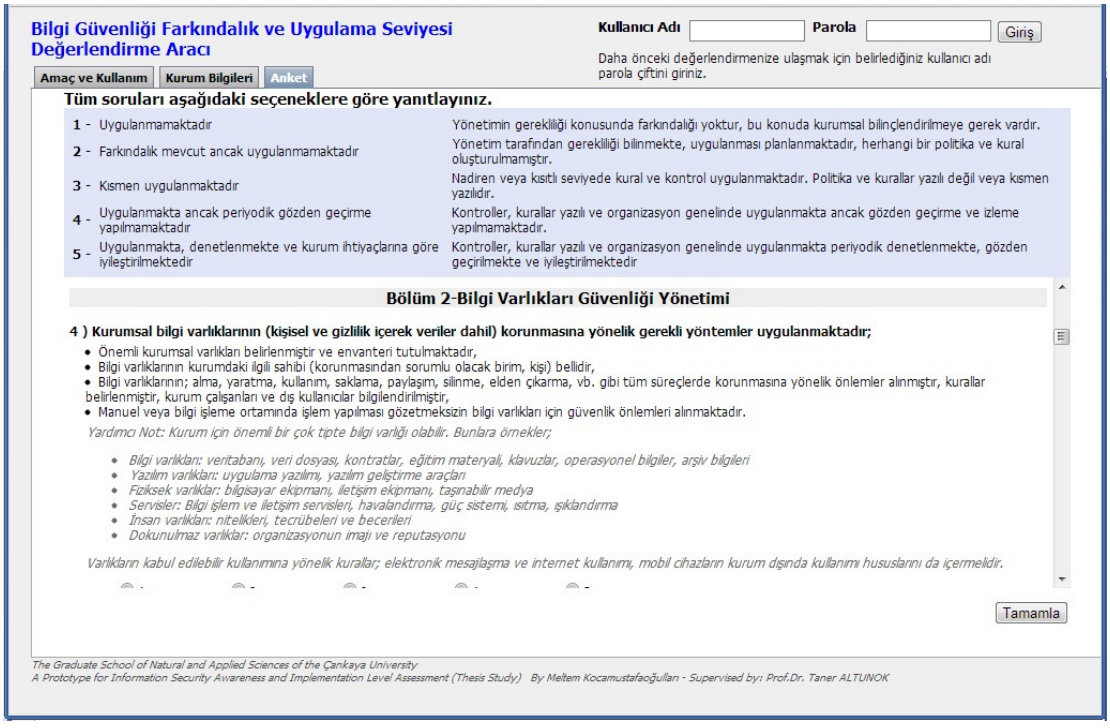


Figure 15. Assessment Questions Module-Section 2

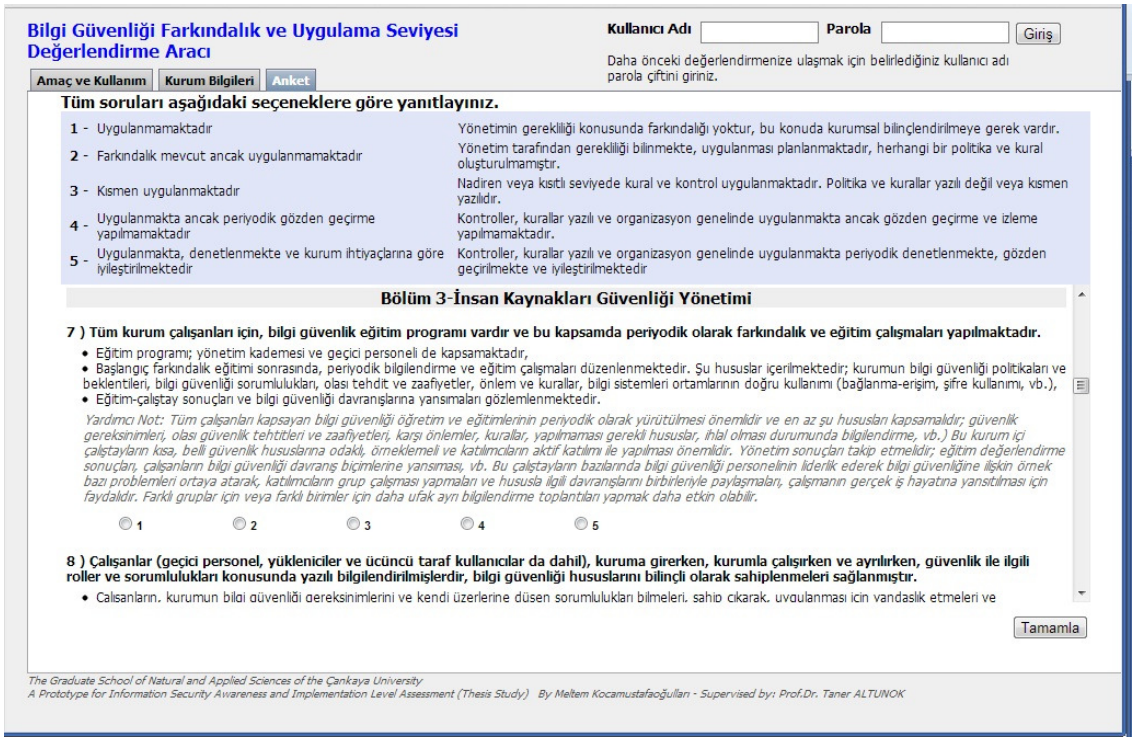


Figure 16. Assessment Questions Module-Section 3

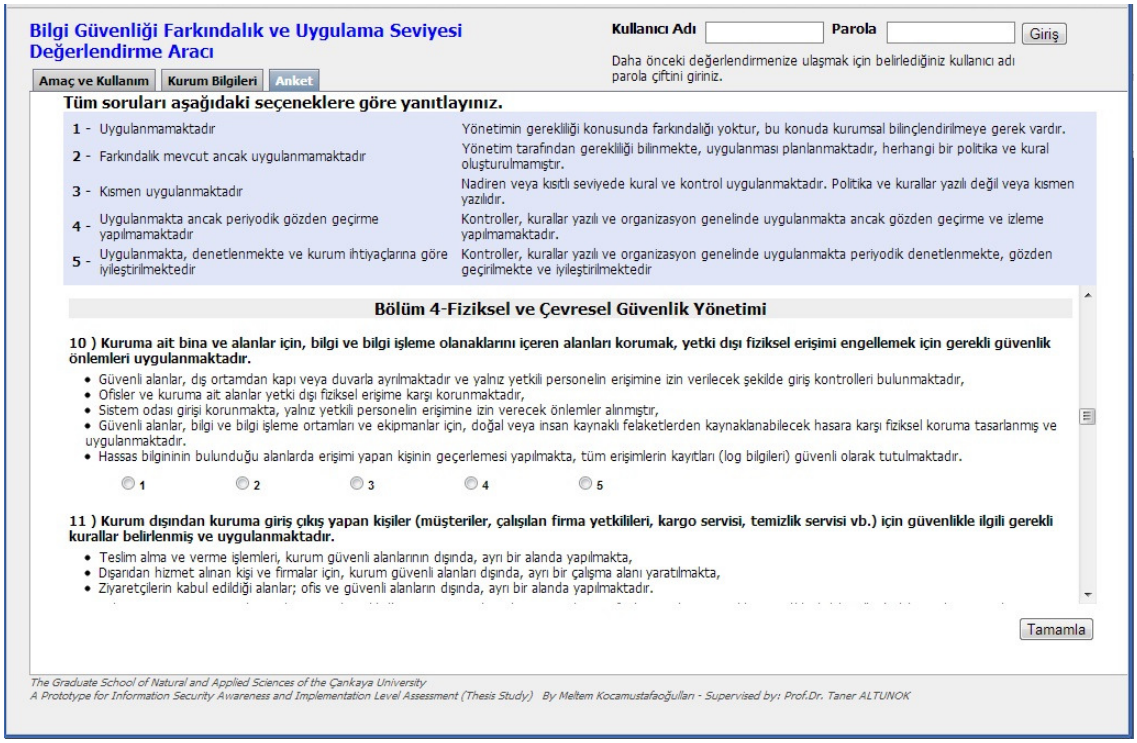


Figure 17. Assessment Questions Module-Section 4

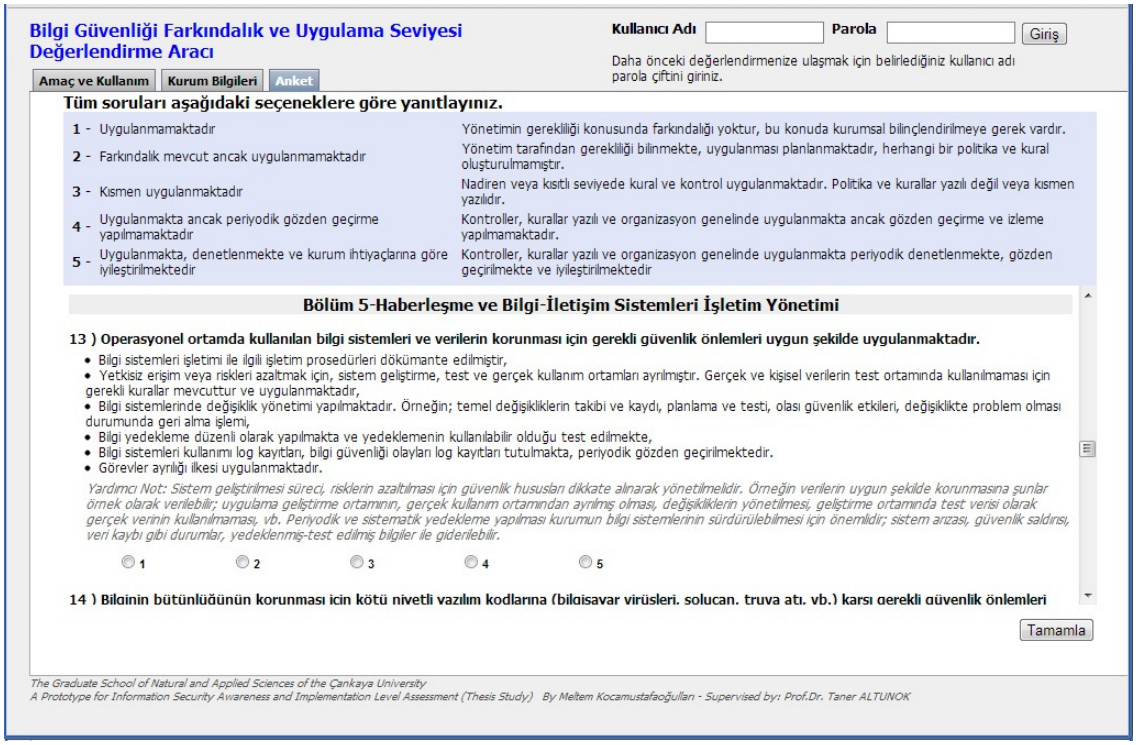


Figure 18. Assessment Questions Module-Section 5

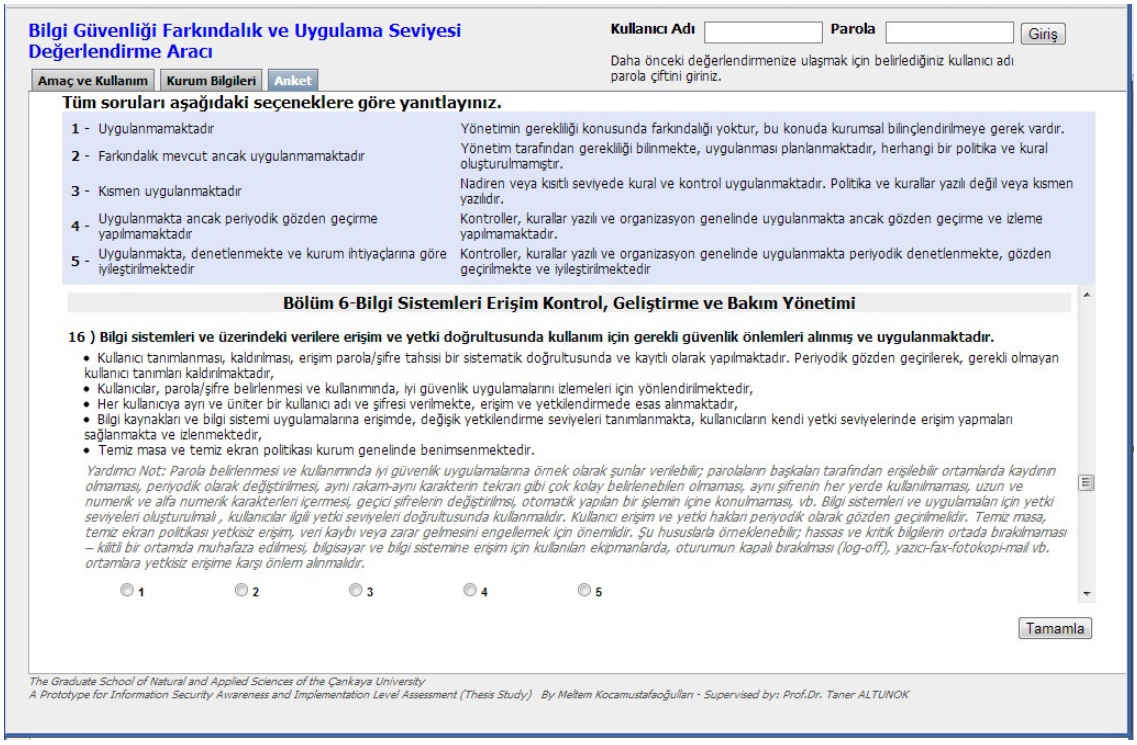


Figure 19. Assessment Questions Module-Section 6

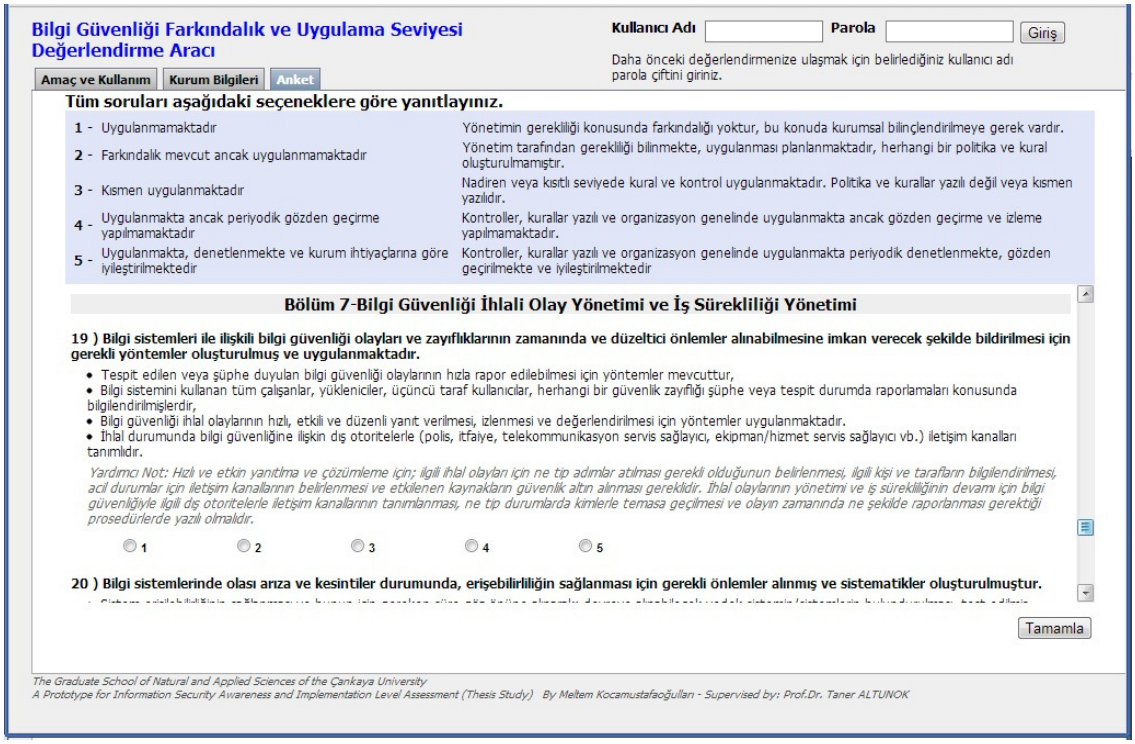


Figure 20. Assessment Questions Module-Section 7

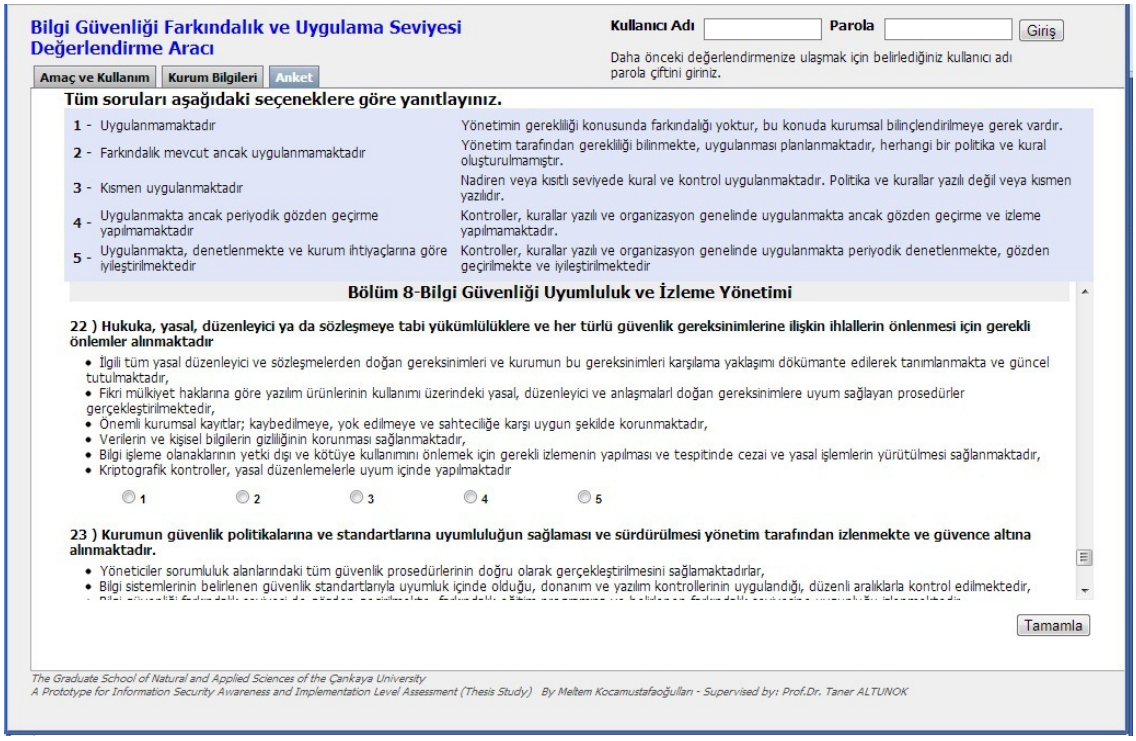


Figure 21. Assessment Questions Module-Section 8

4.4.5. Assessment Results Module

When the user completes the assessment and presses the complete button ("Tamamla") fourth tab is formed to access the assessment results ("Sonuç") module interface. The tab is created for the first time user whereas if the user is accessing the previous assessment record, the tab already appears to show the earlier assessment results. The user can scroll up and down within the pages. Sample test user results are provided below.

The results are placed in a table with short description of the question and the relevant score of the item. The scoring scale is placed above the table for ease of reference. The selected group if given the name of the organization are provided at the top as shown in Figure 22.

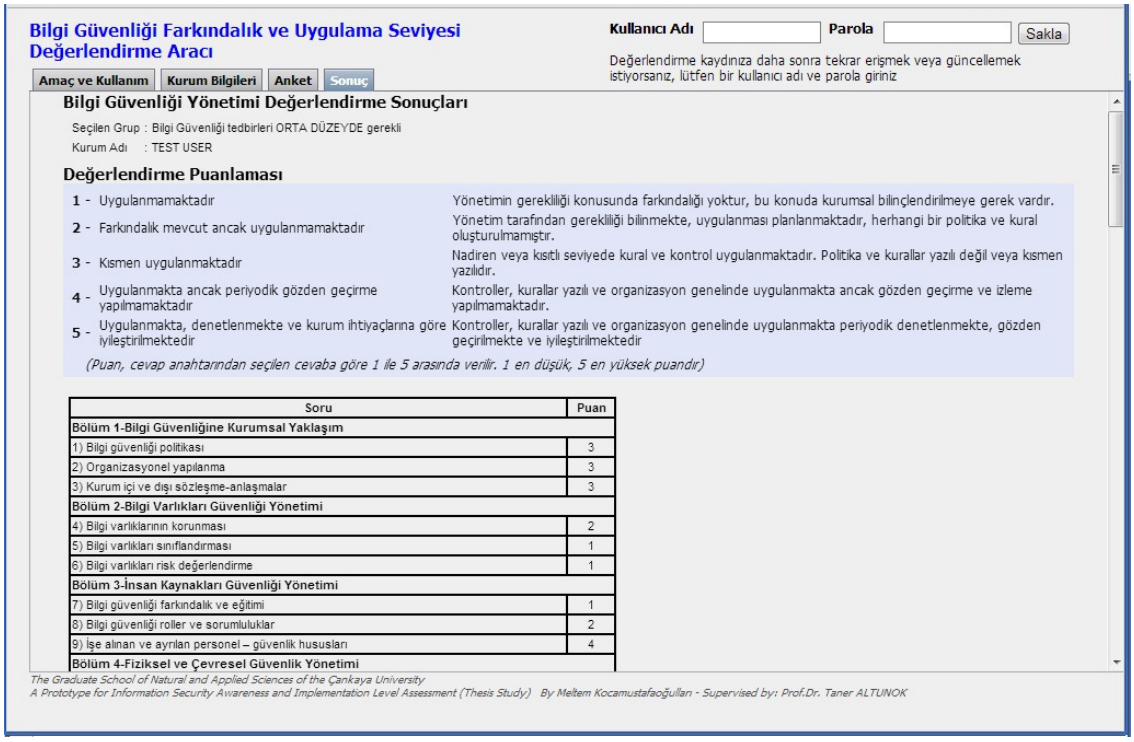


Figure 22. Assessment Results Module - Score Table

Scrolling through the results, summary of the score table is placed at the bottom of the table. Scoring 5 at each question would result with 120. The summary shows the total of the score of the items in comparison to 120. It also shows the average score of the assessment items. The summary table also includes the benchmarking values

belonging to the specific group; the ideal value and the average value from the benchmarking information in the database pre-set based on the expert view. A sample screen is given in Figure 23. This approach is explained in chapter 3.

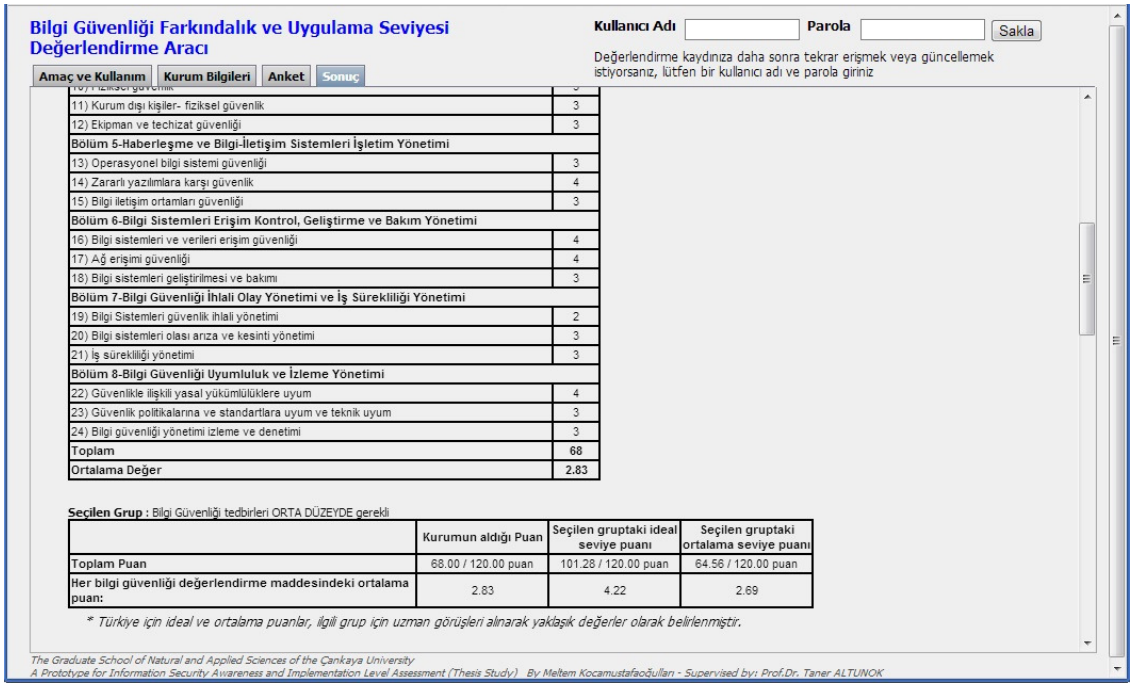


Figure 23. Assessment Results Module - Score Table Summary

Scrolling through the results, the radar graphic presentation is shown. A sample screen is given in Figure 24. Short descriptions of the questions are given. The ideal values of the selected group is shown with red color, the average values of the selected group is shown with black color and the values of the organization are shown with blue color. The radar graphic representation has been used to clearly demonstrate to the user the status and items for improvement as well as relevance to the ideal and average.

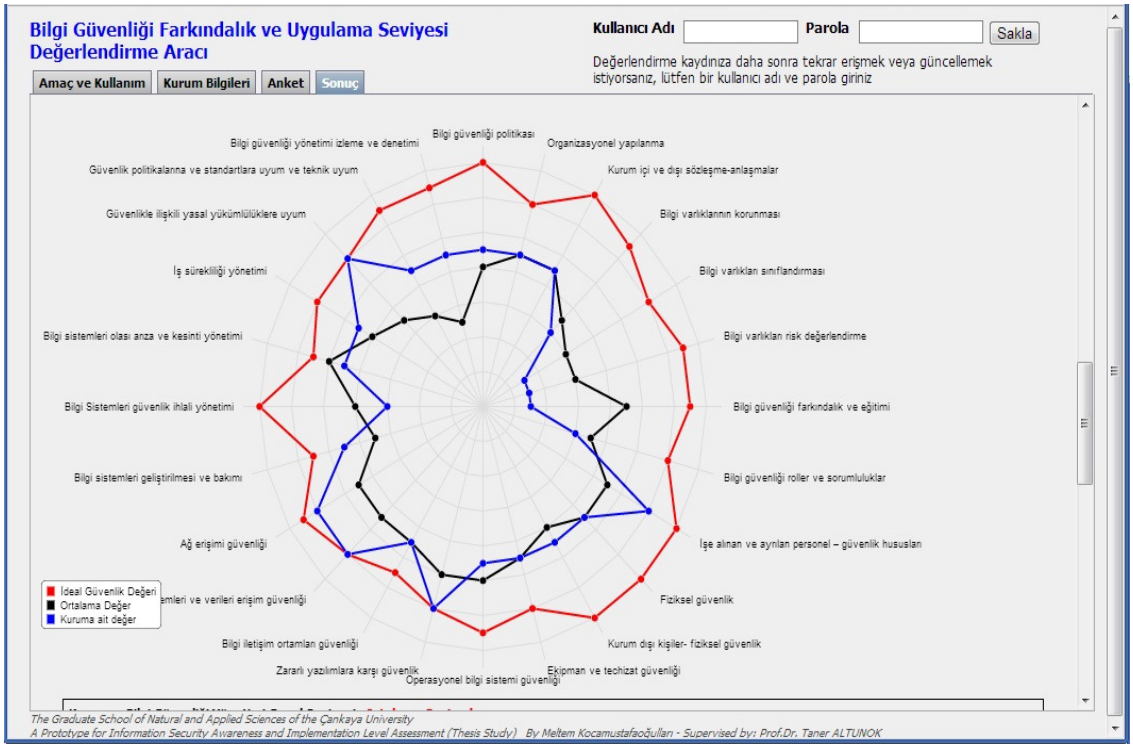


Figure 24. Assessment Results Module - Radar Graphic

At the bottom of the radar graphics, summary and recommendation box is presented. Based on the assessment results the overall status of the organization is stated as one of the below:

i. Ideal Level: If the organization's security assessment results are equal or above compared to the ideal level in their respective group.
ii. Average Level: If the organization's security assessment results are equal or above compared to the average level in their respective group.
iii. Below the Average: If the organization's security assessment results are below compared to the average level in their respective group.

Based on one of the result, short recommendation and guidance is displayed accordingly.

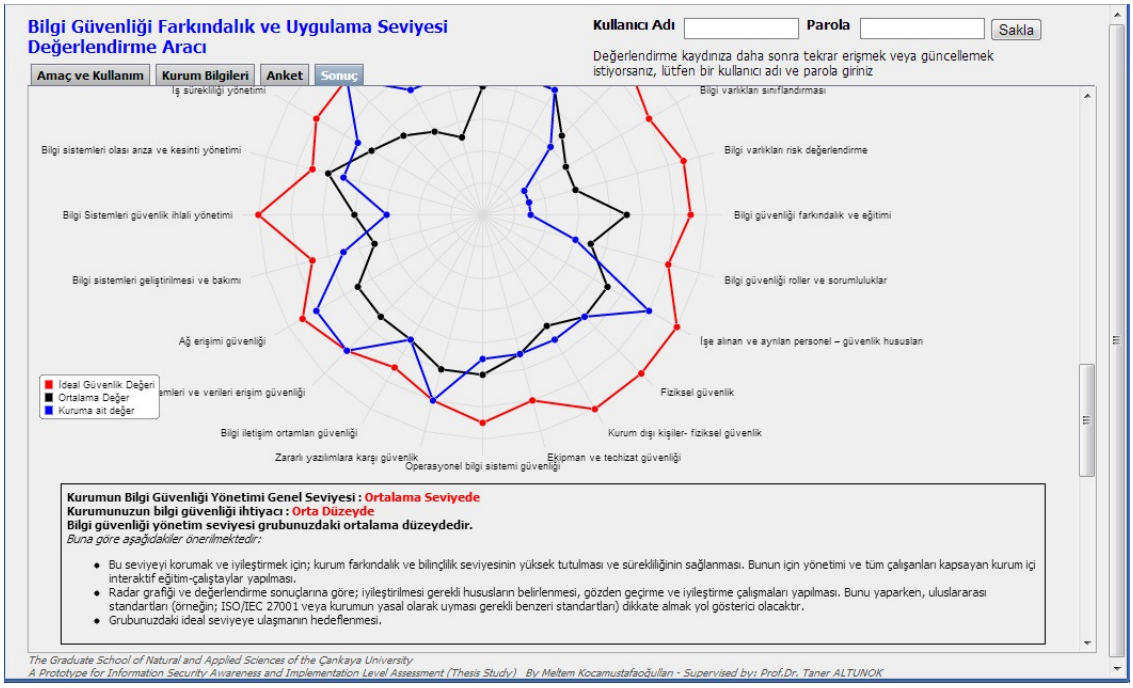


Figure 25. Assessment Results Module - Level and Recommendation

At the bottom of the assessment, a resulting evaluation carnet is provided with a table. Summary of the level is provided for 8 sections in the first table as well as for each security item in the second table as shown in the Figure 26.

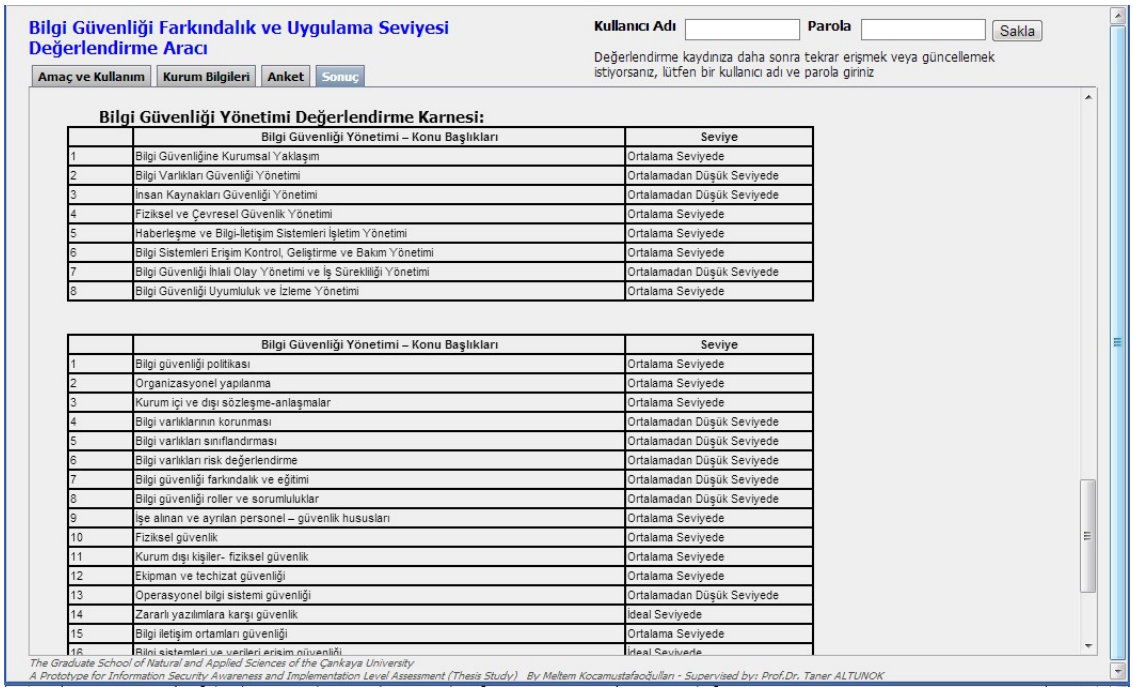


Figure 26. Assessment Results Module – Evaluation Carnet

The results of the assessment can be printed by using print button (“Yazdir”) at the very bottom of the screen. The result can also be saved to a file in pdf format.

4.5. TESTING AND UTILIZATION

For testing of the tool, possible test users need to be identified. In order to test user for the three different groups, test users with different level of security requirements would be preferred as well as organizations from different sectors and sizes. With this consideration, invitation and personal contact has been done to many organizations. The biggest difficulty was inability to have large number of voluntary test users, mainly due to the nature and sensitivity of the topic. These organizations preferred not to conduct the assessment.

In order to progress, personal inquiry has been made to contact own network of organizations and very selective range of organizations have been identified. They have used the tool for the awareness and implementation level assessment of their organizations. In all of the test users the assessment was conducted by the people at management level; most of them having good knowledge on information security and information technologies due to their position and background. Two of the test users were exceptions; who do not have information security knowledge or background. It has been confirmed with the organizations that their names will not be disclosed in the study but only their selected group, field of activity and size information.
Information regarding the twelve test user organizations are provided in the Table 13 including; selected security group, field of activity and the organization’s size.

Table 13. List of Test Users

Number	Group	NACE Code	Field of Activity - Sector Information	Size
1	1	J	INFORMATION AND COMMUNICATION	L
2	1	O	PUBLIC ADMINISTRATION	L
3	1	O	PUBLIC ADMINISTRATION	L
4	1	K	FINANCIAL AND INSURANCE ACTIVITIES	L
5	1	M	PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES	S
6	2	M	PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES	S
7	3	J	INFORMATION AND COMMUNICATION	S
8	3	J	INFORMATION AND COMMUNICATION	S
9	1	J	INFORMATION AND COMMUNICATION	S
10	2	P	EDUCATON	M
11	2	P	EDUCATON	S
12	2	J	INFORMATION AND COMMUNICATION	S

In order to review the assessment results of the test users, the benchmark values for each group needs to be re-addressed. Based on the expert consultation, the benchmark values for each group that are pre-set in the database are given in Table 14.

Table 14. Benchmark Values of the Different Groups

	High Security Measures are Required		MEDIUM LEVEL Security Requirements		LOW LEVEL Security Requirements	
	Group-1 Average	Group-1 Ideal	Group-2 Average	Group-2 Ideal	Group-3 Average	Group-3 Ideal
Total	88.33	118.00	64.67	101.33	44.67	71.00
Average score/item	3.68	4.92	2.69	4.22	1.86	2.96

Review of assessment results for organizations belonging to Group-1 and having high level of security countermeasure requirements are given in Table 15.

Table 15. Assessment Results for Group-1 Organizations

High Security Measures are Required		Number of the Organization						**Avg.of Organizations**
Group-1 Average	Group-1 Ideal	1	2	3	4	5	9	
88,33	118,00	107	119	61	120	66	120	**98.83**
3.68	4.92	4.46	4.96	2.54	5.00	2.75	5.00	**4.12**
	Overall Level:	Mid Level	Ideal Level	Lower than Average	Ideal Level	Lover than Average	Ideal Level	**Mid Level**

Review of assessment results for organizations belonging to Group-2 and having medium level of security countermeasure requirements are given in Table 16.

Table 16. Assessment Results for Group-2 Organizations

Medium Security Measures are Required		Number of the Organization				**Avg.of Organizations**
Group-2 Average	Group-2 Ideal	6	10	11	12	
64.67	101.33	77	68	66	68	**69.75**
2.69	4.22	3.21	2.83	2.75	2.83	**2.90**
	Overall Level:	Mid Level	Mid Level	Mid Level	Mid Level	**Mid Level**

Review of assessment results for organizations belonging to Group-2 and having low level of security countermeasure requirements are given in Table 17.

Table 17. Assessment Results for Group-3 Organizations

Medium Security Measures are Required		Number of the Organization		**Avg.of Organizations**
Group-3 Average	Group-3 Ideal	7	8	
44.67	71.00	83	78	**80.5**
1.86	2.96	3.46	3.25	**3.35**
	Overall Level:	Ideal Level	Ideal Level	**Ideal Level**

The assessment results and details of test user organizations are provided in the appendices to this report (APPENDIX C).

4.6. EVALUATION OF THE TEST RESULTS

The overall evaluation is that;

i. The assessment model and tool has been tested and the tool properly operates.

ii. It has been found useful for organizations having different information security requirements.

iii. All test user organizations believed that such tool can support to have positive impact for awareness-raising on information security at management level as well as SME organizations with low awareness level on the subject.

iv. Test users agree that self-assessment facilitates environment for organizations to objectively and sincerely evaluate their own status.

v. Test users found the presentation of the results understandable and useful for self assessment regarding information security management.

vi. Benchmark has been a motivating factor in the assessment result.

vii. Radar graphic was well selected presentation of the result. Additional graphical presentation can also be useful to add.

Test user assessment results have been reviewed. Regarding the test users under Group-1; all are large scale organizations except number 9. Organizations 2, 4 and 9 have scored ideal level. All three have legal obligations for compliance due to their sector or they already have certification for information security and they have obligation to be in compliance with the relevant standard. One of them is ISO/IEC 267001 certified and another has COBIT compliance. Organization 9 has certification and also obligated to comply with security standards in their sector which is pre-requisite to provide service. Organization 2 identified one IS section that can be further improved which is Communications and Information Systems Operations Management. Organizations 4 and 9 have resulted with all the issues scoring highest 5. Although they may be in compliance with security standards, they may have overestimated their situation since no issues are identified which could be

improved. Organization 1 plans to get information security certification and has used to tool to identify which IS items can be given priority for improvement. Organization 3 which is large scale public authority with established IT department. IT department is well aware of their security requirements and in the process of establishment of information security management system. This organization has sincerely reflected the existing situation which made the average of this group more realistic.

Regarding the test users under Group-2; none of them have security compliance obligations. Two of them are small scale organizations having premises at technology centers. One of them, organization 12, is already aware the security requirements yet identified important security issues that need improvement based on the assessment result. Organization 6, filled the assessment at management level and provided the feedback that the tool was useful to raise awareness on information security issues and to identify own needs to focus for improvement. Organization 12 has conducted the assessment at management level by user having information technology background and based on the result of the tool decided to initiate information security improvement project within the organization. Both organization 10 and 11 are users from education sector and made use of the results as overall assessment of their implementation level and decided to further investigate the items that need to be improved.

Regarding the test users under Group-3; the two test user organizations have low requirement to take information security measures. They both do not have security compliance obligation. They both are small scale and are in information and communication sector and having premises at technology centre. They are very aware of their security requirements and the relevant security measures. They have found their assessment result very useful to re-assure that their current implementation level is sufficient for their specific requirements yet there are topics which can be improved which are currently score below the average.

CHAPTER V

CONCLUSION

The importance of information security management is very evident in today's working environment and it will continue to be. No matter the type, size and nature every organization, based on its own requirements, needs to be aware and establish own procedures and countermeasures to protect their valuable information assets. The weakest cycle is human factor and improving the awareness and ownership has positive impact in strengthening the capacity of the organization concerning information security. Especially commitment and ownership of management makes this evolvement more efficient and applicable. Information security certification records show that Japan is far ahead of its followers and also UK and India also have quite good numbers. The situation in Turkey has improved impressively in last couple of years mainly due to legal compliance requirements and raising awareness both in public and private authorities. Yet improvement is needed especially for the SME sized organizations that are not willing to invest time or resource into information security due to lack of awareness or with preconception of complexity.

The objectives of this thesis are achieved;

i. Prototype model and tool is implemented for organization's self assessment of information security awareness and implementation level,
ii. The tool is implemented to serve as reference point for organizations in building their security requirements and objectives as well as monitoring own overall progress,
iii. A self explanatory web-based tool is facilitated based on ISO/IEC 27001 and ISO/IEC 27002 international security standards and covering essential and common practice security topics and addressing wide range of users without the need for prior training or in-depth technical knowledge on information security,

iv. Benchmark values are provided for organization to compare self status with other organizations having similar information security requirements,

v. The tool is implemented with Turkish user interface in order to contribute for improvement of information security awareness and implementation among Turkish organizations.

The model and tool is tested by experts having solid professional background on information security as well as selective users in Turkey from various sectors such as finance, public authorities, consulting companies and education. The feedback and results verified that the objectives of the thesis are achieved and the tool can serve to improve information security awareness and implementation level of the target users and improve understanding at management level.

The output tool of the thesis is planned to be maintained to sustain its continuity of utilization.

Due to sensitivity of the subject nature, it would be much more efficient if it can be supported by a non profit organization or public authority related with information security. In such case, it can be disseminated to large user base and more organizations can benefit from its results.

The model and tool can have further enhancement such as the following:

i. The benchmark values are defined with limited number of expert consultation. These values can be further enhanced by inviting organizations to use the tool for specific period of time then the values can be used as basis of benchmark. These values can replace the existing pre-set values in the database. Afterwards, the tool can be opened again for utilization of its users for self-assessment.

ii. The assessment is currently benchmarking with organizations belonging to the specific group. Further detail benchmarking can be possible at field of activity basis if the information can be collected at sector basis when establishing invitation based benchmarking values to be set in the database. This can enable sector based status evaluation on information security.

iii. The model and tool incorporates useful tips at the bottom of questions, to provide guidance to the user on the specific topic. These tips can be further enhanced with more text or having link to explanatory and supportive presentations or graphics.

iv. The model and tool is limited to eight sections and twenty four questions. Number of questions can be extended provided that simplicity is preserved for the targeted user base.

v. Further graphical representations such as bar chart can be used to present the analysis of the assessment results.

vi. Currently user decides which group it belongs to in terms of information security measures required. This can be further enhanced by having pre-assessment questions which can based on the answers determine the group of the user.

LIST OF REFERENCES

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

[2] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[3] ISO/IEC27000:2012(E) Information technology - Security techniques - Information security management systems — Overview and vocabulary

[4] H.A.Kruger, W.D.Kearney, (2006). "A Prototype for assessing information security awareness". Science Direct Journal: Computers & Security

[5] Stambul, R.Razali, (2011), "An Assessment Model of Information Security Implementation Levels", International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia

[6] ISO/IEC 20000-1:2011 Information technology – Service management-Part1: Service management system requirements, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51986, on 10th May 2013

[7] COBIT 5: A Business Framework for the Governance and Management of Enterprise IT http://www.isaca.org/COBIT/, on 10th May 2013

[8] About ITIL, http://www.itil-officialsite.com/, on 10th May 2013

[9] V.Fomin, H.J. Vries, Y.Barlette (2008) "ISO/IEC 27001 Information Systems Security Management Standard: Exploring The Reasons For Low Adoption", http://www.techrepublic.com/whitepapers/isoiec-27001-information-systems-security-management-standard-exploring-the-reasons-for-low-adoption/1387721, on 7th January 2013

[10] ISO/IEC 27001:2005 Information technology- Security techniques – Information security management systems – Requirements, http://www.iso27001security.com/html/27001.html, on 12th May 2013

[11] The history of ISO/IEC 27001, Gamma Secure Systems Limited, http://www.gammassl.co.uk/27001/history.php on 12th May 2013

[12] A.Calder (2009) Information Security based on ISO 27001/ISO 27002 – A Management Guide (pp.12, 23–25) Van Haren Publishing

[13] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management, http://www.iso27001security.com/html/27002.html, on 12th May 2013

[14] "International Register of ISMS Certificates", www.iso27001certificates.com/, on 25th April 2013

[15] Turkish Standards Institution “Standart Satış ve Enformasyon” http://www.tse.org.tr/hizmetlerimiz/standart-hizmetleri/standart-satış-ve-enformasyon, on 13th April 2013.

[16] ISMart, Biznet, http://www.biznet.com.tr/en/ismart, on 5th April 2013

[17] INVENTO R&D Software, Invento Information Risk Management Solutions, http://www.invento.com.tr/eng/r_d_software.html, on 5th April 2013

[18] Information Security Awareness Training project General Information, TUBİTAK BİLGEM, http://www.bilgimikoruyorum.org.tr/?icindekiler, on 5th March 2013

[19] Deloitte in association with EMC^2, (July 2012) Irish Information Security and Cybercrime Survey A closer look

[20] PwC The Global State of Information Security Survey 2013, “Explore the data”, http://www.pwc.com/gx/en/consulting-services/information-security-survey/giss.jhtml, on 2nd March 2013

[21] E.Y.Yildirim, G.Akalp, S.Aytac, N.Bayram (2010) Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey, International Journal of Information Management

[22] Prolexic Quarterly Global Distributed Denial of Service Attack Report Q2 2012, Prolexic, http://www.prolexic.com/knowledge-center-dos-and-ddos-attack-reports.html, on 6th April 2013

[23] Y. Kanno, "Information Security Measures Benchmark (ISMBenchmark), "http://www.ipa.go.jp/security/english/benchmark/documents/About_ISM_Benchmark.pdf, on 5th February 2013

[24] PwC the Global State of Information Security Survey 2013, “Benchmark your organization”, http://www.pwc.com/gx/en/consulting-services/information-security-survey/benchmark.jhtml, on 2nd March 2013

[25] D.Milicevic, M.Goeken (2011) Application of Models in Information Security Management, IT-Governance-Practice Network Frankfurt School of Finance and Management Frankfurt am Main, Germany, Published in Research Challenges in Information Science (RCIS), Fifth International Conference on May 2011, http://ieeexplore.ieee.org/, on 11th February 2013

[26] H.Alderfer, S.Flynn, B.Birchmeier, E.Schulz (12/6/2009) Information Policy Country Report: Turkey, Prepared for SI507: Foundations of Information Policy Analysis and Design, School of Information University of Michigan

[27] Resmi İstatistik Programı 2012-2016, TÜİK, Yayın No: 3646, http://www.tuik.gov.tr/rip/doc/II_RIP_2012-2016_04012012.pdf, on 8th January 2013

[28] Turkish Statistical Institute Classification Server, http://tuikapp.tuik.gov.tr/DIESS/SiniflamaSurumListeAction.do?turId=1&turAdi=%201.%20Faaliyet%20S%C4%B1n%C4%B1flamalar%C4%B1, on 9th January 2013

[29] NACE Rev.2, European Commission Eurostat, http://ec.europa.eu/eurostat/ramon/index.cfm?TargetUrl=DSP_PUB_WELC&StrLanguageCode=EN on 12th January 2013

[30] Radar Chart, ASQ, http://asq.org/service/body-of-knowledge/tools-radar-chart on 4th January 2013

APPENDIX A

EXPERT ASSESMENT RESULTS

Expert-1 Assessment Results

Expert View 1

Sectors Covered: J: Information and Communication, K: Financial and Insurance Activities, M: Professional, Scientific and Technical Activities, O: Public Administration and Defense; Compulsory Social Security

Group-1 Average		Group-1 Ideal		Group-2 Average		Group-2 Ideal		Group-3 Average		Group-3 Ideal	
Q	S	Q	S	Q	S	Q	S	Q	S	Q	S
1	5,00	1	5,00	1	3,00	1	5,00	1	1,00	1	3,00
2	5,00	2	5,00	2	3,00	2	4,00	2	1,00	2	2,00
3	5,00	3	5,00	3	3,00	3	5,00	3	1,00	3	3,00
4	5,00	4	5,00	4	2,00	4	4,00	4	1,00	4	2,00
5	4,00	5	5,00	5	2,00	5	4,00	5	1,00	5	2,00
6	4,00	6	5,00	6	2,00	6	5,00	6	1,00	6	3,00
7	5,00	7	5,00	7	3,00	7	4,00	7	1,00	7	3,00
8	4,00	8	5,00	8	2,00	8	4,00	8	1,00	8	3,00
9	4,00	9	5,00	9	3,00	9	5,00	9	3,00	9	4,00
10	5,00	10	5,00	10	3,00	10	5,00	10	3,00	10	4,00
11	4,00	11	5,00	11	3,00	11	5,00	11	3,00	11	4,00
12	4,00	12	5,00	12	3,00	12	4,00	12	3,00	12	4,00
13	3,00	13	5,00	13	3,00	13	4,00	13	3,00	13	3,00
14	4,00	14	5,00	14	3,00	14	4,00	14	3,00	14	4,00
15	3,00	15	5,00	15	3,00	15	3,00	15	3,00	15	3,00
16	5,00	16	5,00	16	3,00	16	4,00	16	3,00	16	4,00
17	5,00	17	5,00	17	3,00	17	4,00	17	3,00	17	4,00
18	3,00	18	5,00	18	2,00	18	3,00	18	2,00	18	3,00
19	4,00	19	5,00	19	3,00	19	5,00	19	2,00	19	4,00
20	5,00	20	5,00	20	3,00	20	3,00	20	3,00	20	3,00
21	4,00	21	5,00	21	3,00	21	4,00	21	3,00	21	2,00
22	3,00	22	5,00	22	3,00	22	4,00	22	3,00	22	3,00
23	3,00	23	5,00	23	2,00	23	4,00	23	1,00	23	3,00
24	5,00	24	5,00	24	2,00	24	4,00	24	1,00	24	3,00

(Q: Question, S: Score)

Expert-2 Assessment Results

Expert View 2

Sectors Covered: C: Manufacturing, H: Transportation and Storage, O: Public Administration and Defense; Compulsory Social Security

Group-1 Average		Group-1 Ideal		Group-2 Average		Group-2 Ideal		Group-3 Average		Group-3 Ideal	
Q	S	Q	S	Q	S	Q	S	Q	S	Q	S
1	5,00	1	5,00	1	3,00	1	5,00	1	1,00	1	3,00
2	5,00	2	5,00	2	4,00	2	5,00	2	2,00	2	2,00
3	5,00	3	5,00	3	4,00	3	5,00	3	3,00	3	3,00
4	5,00	4	5,00	4	3,00	4	5,00	4	2,00	4	2,00
5	4,00	5	5,00	5	3,00	5	5,00	5	1,00	5	2,00
6	4,00	6	5,00	6	3,00	6	5,00	6	1,00	6	3,00
7	5,00	7	5,00	7	4,00	7	5,00	7	2,00	7	3,00
8	4,00	8	5,00	8	3,00	8	5,00	8	1,00	8	3,00
9	4,00	9	5,00	9	4,00	9	5,00	9	1,00	9	4,00
10	5,00	10	5,00	10	4,00	10	5,00	10	3,00	10	4,00
11	4,00	11	5,00	11	3,00	11	5,00	11	3,00	11	4,00
12	4,00	12	5,00	12	4,00	12	5,00	12	3,00	12	4,00
13	3,00	13	5,00	13	5,00	13	5,00	13	3,00	13	3,00
14	4,00	14	5,00	14	5,00	14	5,00	14	4,00	14	4,00
15	3,00	15	5,00	15	4,00	15	5,00	15	3,00	15	3,00
16	5,00	16	5,00	16	4,00	16	5,00	16	3,00	16	4,00
17	5,00	17	5,00	17	4,00	17	5,00	17	3,00	17	4,00
18	3,00	18	5,00	18	4,00	18	5,00	18	3,00	18	3,00
19	4,00	19	5,00	19	3,00	19	5,00	19	3,00	19	4,00
20	5,00	20	5,00	20	5,00	20	5,00	20	3,00	20	3,00
21	4,00	21	5,00	21	3,00	21	5,00	21	2,00	21	2,00
22	3,00	22	5,00	22	3,00	22	5,00	22	2,00	22	3,00
23	3,00	23	5,00	23	3,00	23	5,00	23	1,00	23	3,00
24	5,00	24	5,00	24	1,00	24	5,00	24	1,00	24	3,00

(Q: Question, S: Score)

Expert-3 Assessment Results

Expert View 3

Sectors Covered: C: Manufacturing, H: Transportation and Storage, J: Information and Communication,M: Professional, Scientific and Technical Activities

Group-1 Average		Group-1 Ideal		Group-2 Average		Group-2 Ideal		Group-3 Average		Group-3 Ideal	
Q	S	Q	S	Q	S	Q	S	Q	S	Q	S
1	3,00	1	5,00	1	2,00	1	4,00	1	1,00	1	2,00
2	3,00	2	5,00	2	2,00	2	3,00	2	1,00	2	1,00
3	3,00	3	5,00	3	2,00	3	4,00	3	1,00	3	3,00
4	2,00	4	5,00	4	2,00	4	4,00	4	1,00	4	1,00
5	2,00	5	5,00	5	1,00	5	3,00	5	1,00	5	1,00
6	2,00	6	4,00	6	1,00	6	3,00	6	1,00	6	2,00
7	2,00	7	5,00	7	2,00	7	4,00	7	1,00	7	3,00
8	3,00	8	4,00	8	2,00	8	3,00	8	1,00	8	2,00
9	3,00	9	4,00	9	2,00	9	4,00	9	1,00	9	3,00
10	3,00	10	5,00	10	2,00	10	4,00	10	2,00	10	3,00
11	2,00	11	5,00	11	2,00	11	4,00	11	2,00	11	3,00
12	3,00	12	5,00	12	2,00	12	3,00	12	2,00	12	3,00
13	3,00	13	5,00	13	2,00	13	4,00	13	1,00	13	3,00
14	3,00	14	5,00	14	2,00	14	3,00	14	2,00	14	3,00
15	3,00	15	5,00	15	2,00	15	3,00	15	1,00	15	3,00
16	3,00	16	5,00	16	2,00	16	3,00	16	1,00	16	3,00
17	3,00	17	5,00	17	2,00	17	4,00	17	2,00	17	3,00
18	2,00	18	4,00	18	1,00	18	3,00	18	1,00	18	3,00
19	2,00	19	5,00	19	2,00	19	4,00	19	1,00	19	3,00
20	4,00	20	5,00	20	2,00	20	3,00	20	2,00	20	3,00
21	2,00	21	4,00	21	2,00	21	3,00	21	1,00	21	2,00
22	2,00	22	4,00	22	1,00	22	3,00	22	1,00	22	2,00
23	2,00	23	5,00	23	1,00	23	4,00	23	1,00	23	3,00
24	3,00	24	5,00	24	2,00	24	4,00	24	1,00	24	3,00

(Q: Question, S: Score)

Merged Mean Values of Experts To be Used in Benchmarking

Expert Views merged

Sectors Covered: C: Manufacturing, H: Transportation and Storage, J: Information and Communication, K: Financial and Insurance Activities, M: Professional, Scientific and Technical Activities, O: Public Administration and Defense; Compulsory Social Security

Group-1 Average		Group-1 Ideal		Group-2 Average		Group-2 Ideal		Group-3 Average		Group-3 Ideal	
Q	S	Q	S	Q	S	Q	S	Q	S	Q	S
1	4,33	1	5,00	1	2,67	1	4,67	1	1,00	1	2,67
2	4,33	2	5,00	2	3,00	2	4,00	2	1,33	2	1,67
3	4,33	3	5,00	3	3,00	3	4,67	3	1,67	3	3,00
4	4,00	4	5,00	4	2,33	4	4,33	4	1,33	4	1,67
5	3,33	5	5,00	5	2,00	5	4,00	5	1,00	5	1,67
6	3,33	6	4,67	6	2,00	6	4,33	6	1,00	6	2,67
7	4,00	7	5,00	7	3,00	7	4,33	7	1,33	7	3,00
8	3,67	8	4,67	8	2,33	8	4,00	8	1,00	8	2,67
9	3,67	9	4,67	9	3,00	9	4,67	9	1,67	9	3,67
10	4,33	10	5,00	10	3,00	10	4,67	10	2,67	10	3,67
11	3,33	11	5,00	11	2,67	11	4,67	11	2,67	11	3,67
12	3,67	12	5,00	12	3,00	12	4,00	12	2,67	12	3,67
13	3,00	13	5,00	13	3,33	13	4,33	13	2,33	13	3,00
14	3,67	14	5,00	14	3,33	14	4,00	14	3,00	14	3,67
15	3,00	15	5,00	15	3,00	15	3,67	15	2,33	15	3,00
16	4,33	16	5,00	16	3,00	16	4,00	16	2,33	16	3,67
17	4,33	17	5,00	17	3,00	17	4,33	17	2,67	17	3,67
18	2,67	18	4,67	18	2,33	18	3,67	18	2,00	18	3,00
19	3,33	19	5,00	19	2,67	19	4,67	19	2,00	19	3,67
20	4,67	20	5,00	20	3,33	20	3,67	20	2,67	20	3,00
21	3,33	21	4,67	21	2,67	21	4,00	21	2,00	21	2,00
22	2,67	22	4,67	22	2,33	22	4,00	22	2,00	22	2,67
23	2,67	23	5,00	23	2,00	23	4,33	23	1,00	23	3,00
24	4,33	24	5,00	24	1,67	24	4,33	24	1,00	24	3,00

Total	88,33	118,00	64,67	101,33	44,67	71,00
Avg. score/ item	3,68	4,92	2,69	4,22	1,86	2,96

APPENDIX B

ASSESSMENT TOOL IMPLEMENTATION SAMPLE CODES

```
$(document).ready(function () {
      <%

            if (attendeeId != null) {
                  if (attendee != null && attendee.getAttendeeId() != null) {
                        if (attendee.getOrganisationName() != null)
out.write("$('#organisationName').val('"+attendee.getOrganisationName()+"');");
                        if (attendee.getSector() != null)
out.write("$('#sector').val('"+attendee.getSector()+"');");
                        if (attendee.getScale() != null)
out.write("$('#scale').val('"+attendee.getScale()+"');");

      out.write("AgForm.setRadioButtonValue('groupId','"+attendee.getGroupId()+"
');");

                        Collection<AnswerForm> answers =
(Collection<AnswerForm>) request.getAttribute("answers");
                        if (answers != null) {
                              for (AnswerForm ans : answers) {

      out.write("AgForm.setRadioButtonValue('answer_"+ans.getQuestionId()+"','"+
ans.getOptionId()+"');");
                              }
                        }
                  } else {
                        out.write("AgForm.setRadioButtonValue('groupId','1');");
                  }
            } else {
                  out.write("AgForm.setRadioButtonValue('groupId','1');");
            }

            if (attendeeId != null)  {
                if (attendee != null && attendee.getUsername() != null) {
            %>
                        $('#loginDiv').hide();
```

```
Güvenliği Farkındalık ve Uygulama Seviyesi Değerlendirme Aracı</div>
</div>
<div id="tabDivControl" style="position: absolute; left:20px; width:1000px;
height:530px; top:55px">
<div class="tabber">
      <div class="tabbertab" style="position:relative; height:100%; width:100%;
background-color: white;">
            <h2>Amaç ve Kullanım</h2>
            <br/>
            <ul class="isma">
                  <li>Bu uygulamanın amacı, bilgi güvenliği yönetimine yönelik
organizasyonun kendi değerlendirmesini yapabileceği bir ortam yaratmaktır.
Bilgi güvenliği yönetimine yönelik uygulama seviyesinin belirlenmesi ve
iyileştirmeye yönelik  yapılacak planlamada değerlendirilmesi ve temel alınması
hedeflenmiştir.</li>
                  <li>Sorular 6 başlık altında toplanmıştır, sonuç alınabilmesi
için tümü cevaplanmalıdır. Sorular Bilgi Güvenliği Uluslararası standart ISO/IEC
27001:2005 gereksinimleri ve kontrol hedefleri temel alınarak
hazırlanmıştır.</li>
                  <li>Seçilen gruptaki avaraj ve ideal değerler uzman görüşü
alınarak belirlenmiştir. Sonuç değerlendirmede; organizasyonun, avaraj ve ideal
değerlere göre durumu bilgi ve grafik olarak belirtilir. </li>
            </ul>
          <span style="  font-family:Ubuntu,Tahoma,Arial;font-size: 15; font-
weight:bold; margin-left:30px">BGY Değerlendirme Adımları:</span>
            <ul class="isma_numeric">
                  <li>Organizasyonunuza en uygun grubu seçin </li>
                  <li>Tüm belirtilen hususlar için organizasyonunuzun
uygulamalarına yönelik en uygun yanıtı seçin </li>
                  <li>Değerlendirmeyi başlatmadan önce gözden geçirin,
düzeltmeniz varsa yapın </li>
                  <li>Değerlendirme sonucu ekranda html olarak görüntülenir
(saklayabilir veya basabilirsiniz) </li>
            </ul>
      </div>

      <div class="tabbertab" style="position:relative; height:100%; width:100%;
background-color: white;">
            <h2>Kurum Bilgileri</h2>
            <br/>
            <div style="border:1px; background-color:#E0E6F8; margin-left:30px;
```

```
                                        out.write("<td class='optionId
answer'><input type='radio' id='answer_" + q.getQuestionId() + "' name='answer_"
+ q.getQuestionId() + "'
value='"+o.getOptionId()+"'/>"+o.getOptionId()+"</td>");
                                    }
                                    out.write("</tr></table></div>");
                                }
                                out.write("<br/>");
                            }
                        %>
                </div>
                <div style='font-family:Ubuntu,Tahoma,Arial;font-size: 15; font-
weight:bold; margin-top:10px; margin-right:30px; text-align:right'>
                    <button type="button" onclick='finishForm()'>Tamamla</button>
                </div>
        </div>
<% if (attendeeId != null)  {  %>
        <div class="tabbertab" style="position:relative; height:100%; width:100%;
background-color: white;">
                <h2>Sonuç</h2>
                <IFRAME src="assesment/assesment/select.do" style="border: none;
width: 100%; height: 100%;" frameborder="0" name="assesmentAssesment"
id="assesmentAssesment"></IFRAME>
        </div>
<% } %>
</div>
<div style="font-family:Ubuntu,Tahoma,Arial;font-size: 10; font-style:italic;
color:#505050">
The Graduate School of Natural and Applied Sciences of the Çankaya
University<br/>
A Prototype for Information Security Awareness and Implementation Level
Assessment (Thesis Study)  
By Meltem Kocamustafaoğulları  -  Supervised by: Prof.Dr. Taner ALTUNOK <br>
</div>
</div>

</form>
</body>
</html>
```

```
</script>
</head>
<body>
<div class="p_page p_break">
<span style="  font-family:Ubuntu,Tahoma,Arial;font-size: 15; font-weight:bold;
margin-left:30px">Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları </span>
<div style="border:1px; margin-left:30px; margin-right:30px; padding: 5 5 5 5;">
      <table class='organisation'>
      <tbody>
      <%
            out.write("<tr><td>Seçilen
Grup</td><td>:</td><td>"+assesment.getGroupText()+"</td></tr>");
            out.write("<tr><td>Kurum
Adı</td><td>:</td><td>"+assesment.getOrganisationName()+"</td></tr>");
      %>
      </tbody>
      </table>
</div>

<span style="  font-family:Ubuntu,Tahoma,Arial;font-size: 15; font-weight:bold;
margin-left:30px">Değerlendirme Puanlaması </span>
<div style="border:1px; background-color:#E0E6F8; margin-left:30px; margin-
right:30px; padding: 5 5 5 5;">
      <table class='options'>
      <tbody>
      <%
            List<OptionForm> optionList = (List<OptionForm>)
request.getAttribute("optionList");
            for (OptionForm o : optionList)
            {
                  out.write("<tr><td class='optionId'>" + o.getOptionId() +
" -
 </td><td>"+o.getOptionText()+"</td><td>"+o.getExplanation()+"</td></tr>");
            }
      %>
      </tbody>
      </table>
      <div style='font-family:Ubuntu,Tahoma,Arial;font-size: 12; margin-top:5px;
margin-left:15px'><i>(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5
arasında verilir. 1 en düşük, 5 en yüksek puandır)</i></div>
```

```
<div style=" margin-left:30px; margin-right:30px; padding: 5 5 5 5;">
<table cellspacing='0' style='border: 1px solid black;width:500px'>
<thead style='background-color:eee; font-size:15px; padding:none'>
      <tr><th style='border: 1px solid black; width:450px'>Soru</th><th
style='border: 1px solid black; text-align:center'>Puan</th></tr>
</thead>
<tbody>
      <%
            long total = 0L;
            double avrg;
            List<SectionForm> sectionList = (List<SectionForm>)
request.getAttribute("sectionList");
            Collection<Long> attendeeScore= new ArrayList<Long>();
            Collection<Double> idealScore = new ArrayList<Double>();
            Collection<Double> averageScore = new ArrayList<Double>();
            Collection<String> questionName = new ArrayList<String>();
```

```
            for (SectionForm s : sectionList)
            {
                  long sectionTotal = 0;
                  out.write("<tr><td colspan='2' style='border: 1px solid
black'><b>Bölüm "+s.getSectionId()+"-" +s.getSectionText()+"</b></td></tr>");
                  for (QuestionForm q : s.getQuestions())
                  {
                        out.write("<tr><td style='border: 1px solid
black'>"+q.getQuestionId()+") "+q.getShortText()+"</td><td style='border: 1px
solid black; text-align:center'>"+q.getAnswer()+"</td></tr>");
                        total += q.getAnswer();
                        sectionTotal += q.getAnswer();
                        q.setIdealScore(new
Long(1).equals(assesment.getGroupId()) ? q.getIdealScoreG1() : (new
Long(2).equals(assesment.getGroupId()) ? q.getIdealScoreG2()
:q.getIdealScoreG3()));
                        q.setAverageScore(new
Long(1).equals(assesment.getGroupId()) ? q.getAverageScoreG1() : (new
Long(2).equals(assesment.getGroupId()) ? q.getAverageScoreG2()
:q.getAverageScoreG3()));
                        attendeeScore.add(q.getAnswer());
                        idealScore.add(q.getIdealScore());
                        averageScore.add( q.getAverageScore());
                        questionName.add("'" + q.getShortText() + "'");
                  }
                  s.setScore(sectionTotal);
            }
            avrg = (total/24.0);
```

APPENDIX C

ASSESSMENT RESULTS OF THE TEST USERS

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli
Kurum Adı : KURUM 11
Faaliyet Alanı : J-BİLGİ VE İLETİŞİM
Kurum Ölçeği : Büyük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

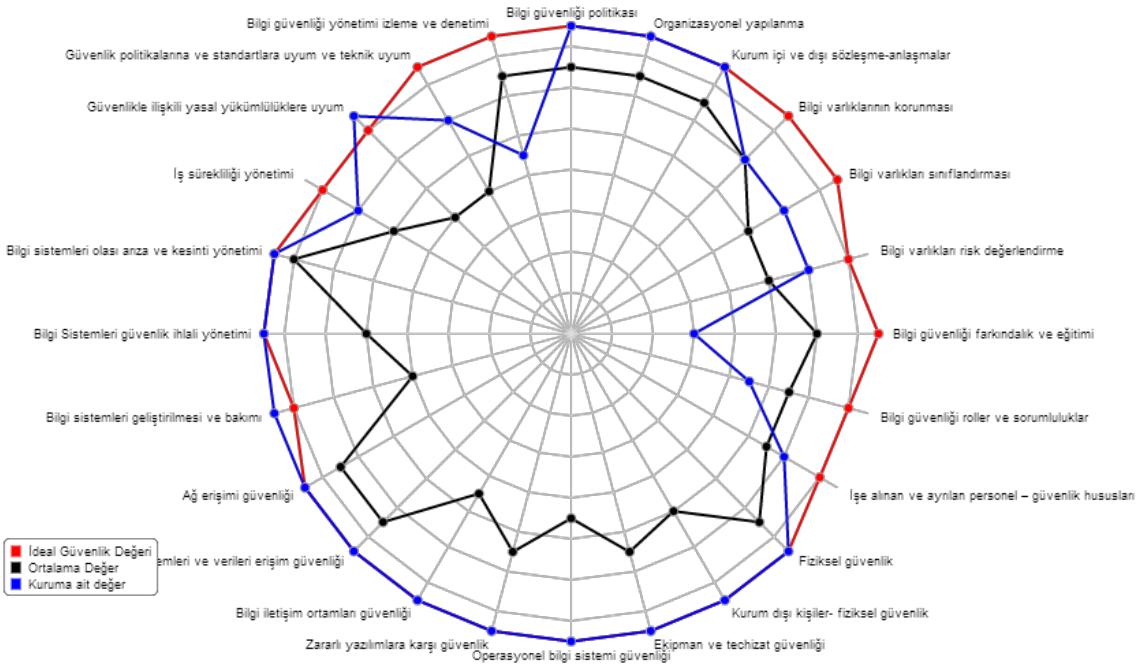
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	5
2) Organizasyonel yapılanma	5
3) Kurum içi ve dışı sözleşme-anlaşmalar	5
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	4
5) Bilgi varlıkları sınıflandırması	4
6) Bilgi varlıkları risk değerlendirme	4
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	2
8) Bilgi güvenliği roller ve sorumluluklar	3
9) İşe alınan ve ayrılan personel – güvenlik hususları	4
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	5
11) Kurum dışı kişiler- fiziksel güvenlik	5
12) Ekipman ve techizat güvenliği	5
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	5
14) Zararlı yazılımlara karşı güvenlik	5
15) Bilgi iletişim ortamları güvenliği	5
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	5
17) Ağ erişimi güvenliği	5
18) Bilgi sistemleri geliştirilmesi ve bakımı	5
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	5
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	5
21) İş sürekliliği yönetimi	4
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	5
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	4
24) Bilgi güvenliği yönetimi izleme ve denetimi	3
Toplam	**107**
Ortalama Değer	**4.46**

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	107.00 / 120.00 puan	118.08 / 120.00 puan	88.32 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	4.46	4.92	3.68

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : Ortalama Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Yüksek Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ortalama düzeydedir.
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyeyi korumak ve iyileştirmek için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştaylar yapılması.
- Radar grafiği ve değerlendirme sonuçlarına göre; iyileştirilmesi gerekli hususların belirlenmesi, gözden geçirme ve iyileştirme çalışmaları yapılması. Bunu yaparken, uluslararası standartları (örneğin; ISO/IEC 27001 veya kurumun yasal olarak uyması gerekli benzeri standartları) dikkate almak yol gösterici olacaktır.
- Grubunuzdaki ideal seviyeye ulaşmanın hedeflenmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	İdeal Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	Ortalama Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	İdeal Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	İdeal Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	İdeal Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	Ortalama Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	Ortalama Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	İdeal Seviyede
2	Organizasyonel yapılanma	İdeal Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	İdeal Seviyede
4	Bilgi varlıklarının korunması	Ortalama Seviyede
5	Bilgi varlıkları sınıflandırması	Ortalama Seviyede
6	Bilgi varlıkları risk değerlendirme	Ortalama Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	Ortalamadan Düşük Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	Ortalamadan Düşük Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	Ortalama Seviyede
10	Fiziksel güvenlik	İdeal Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	İdeal Seviyede
12	Ekipman ve techizat güvenliği	İdeal Seviyede
13	Operasyonel bilgi sistemi güvenliği	İdeal Seviyede
14	Zararlı yazılımlara karşı güvenlik	İdeal Seviyede
15	Bilgi iletişim ortamları güvenliği	İdeal Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	İdeal Seviyede
17	Ağ erişimi güvenliği	İdeal Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	İdeal Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	İdeal Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	İdeal Seviyede
21	İş sürekliliği yönetimi	Ortalama Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	İdeal Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	Ortalama Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	Ortalamadan Düşük Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli
Kurum Adı : KURUM 12
Faaliyet Alanı : O-KAMU YÖNETİMİ VE SAVUNMA; ZORUNLU SOSYAL GÜVENLİK
Kurum Ölçeği : Büyük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

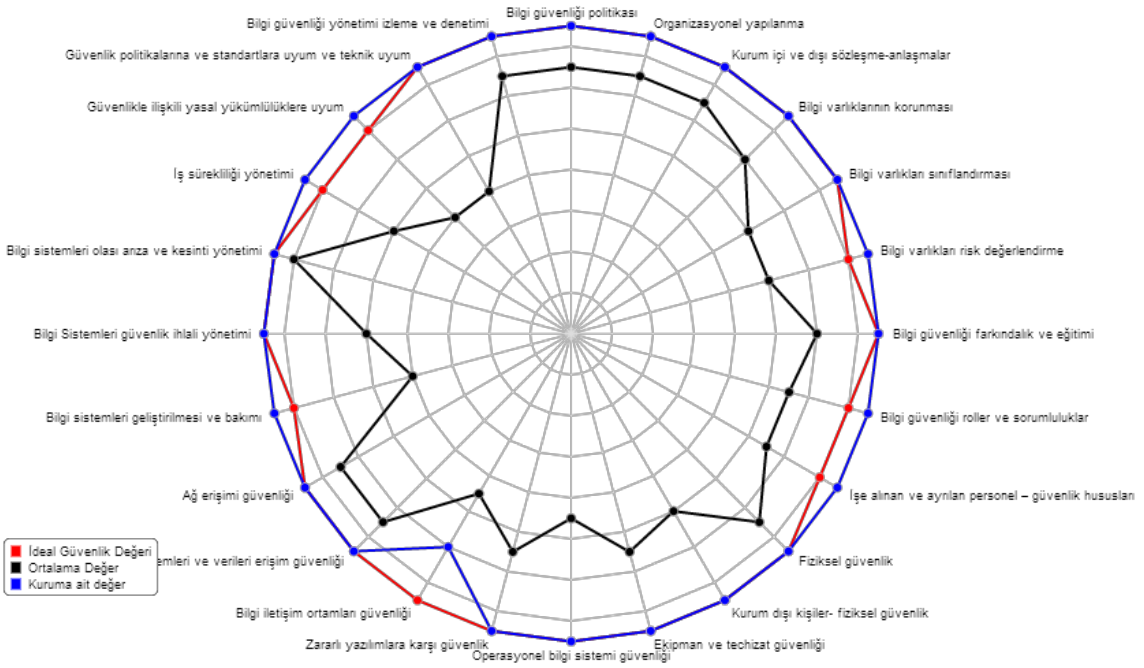
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	5
2) Organizasyonel yapılanma	5
3) Kurum içi ve dışı sözleşme-anlaşmalar	5
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	5
5) Bilgi varlıkları sınıflandırması	5
6) Bilgi varlıkları risk değerlendirme	5
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	5
8) Bilgi güvenliği roller ve sorumluluklar	5
9) İşe alınan ve ayrılan personel – güvenlik hususları	5
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	5
11) Kurum dışı kişiler- fiziksel güvenlik	5
12) Ekipman ve techizat güvenliği	5
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	5
14) Zararlı yazılımlara karşı güvenlik	5
15) Bilgi iletişim ortamları güvenliği	4
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	5
17) Ağ erişimi güvenliği	5
18) Bilgi sistemleri geliştirilmesi ve bakımı	5
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	5
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	5
21) İş sürekliliği yönetimi	5
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	5
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	5
24) Bilgi güvenliği yönetimi izleme ve denetimi	5
Toplam	**119**
Ortalama Değer	**4.96**

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	119.00 / 120.00 puan	118.08 / 120.00 puan	88.32 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	4.96	4.92	3.68

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : İdeal Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Yüksek Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ideal düzeydedir. Tebrikler !
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyenin korunması için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştayların sürdürülmesi.
- İdeal seviyenin korunması için gerekli gözden geçirme ve iyileştirme döngüsünün sürdürülmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	İdeal Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	İdeal Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	İdeal Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	İdeal Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	Ortalama Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	İdeal Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	İdeal Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	İdeal Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	İdeal Seviyede
2	Organizasyonel yapılanma	İdeal Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	İdeal Seviyede
4	Bilgi varlıklarının korunması	İdeal Seviyede
5	Bilgi varlıkları sınıflandırması	İdeal Seviyede
6	Bilgi varlıkları risk değerlendirme	İdeal Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	İdeal Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	İdeal Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	İdeal Seviyede
10	Fiziksel güvenlik	İdeal Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	İdeal Seviyede
12	Ekipman ve techizat güvenliği	İdeal Seviyede
13	Operasyonel bilgi sistemi güvenliği	İdeal Seviyede
14	Zararlı yazılımlara karşı güvenlik	İdeal Seviyede
15	Bilgi iletişim ortamları güvenliği	Ortalama Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	İdeal Seviyede
17	Ağ erişimi güvenliği	İdeal Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	İdeal Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	İdeal Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	İdeal Seviyede
21	İş sürekliliği yönetimi	İdeal Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	İdeal Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	İdeal Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	İdeal Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli
Kurum Adı : KURUM 13
Faaliyet Alanı : O-KAMU YÖNETİMİ VE SAVUNMA; ZORUNLU SOSYAL GÜVENLİK
Kurum Ölçeği : Büyük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

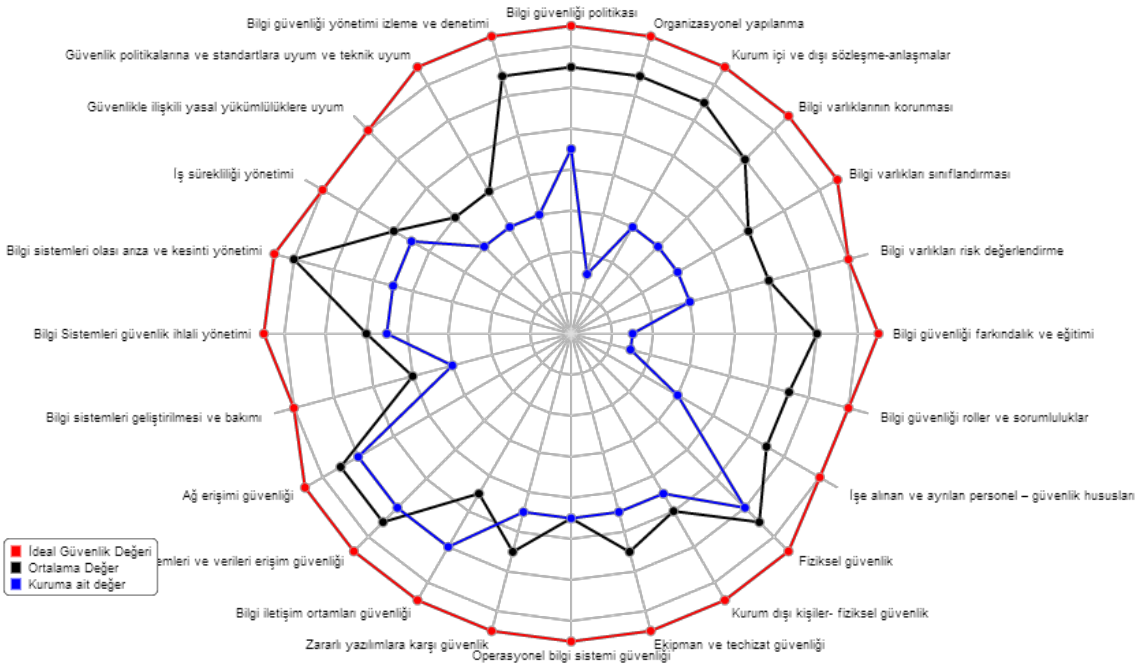
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	3
2) Organizasyonel yapılanma	1
3) Kurum içi ve dışı sözleşme-anlaşmalar	2
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	2
5) Bilgi varlıkları sınıflandırması	2
6) Bilgi varlıkları risk değerlendirme	2
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	1
8) Bilgi güvenliği roller ve sorumluluklar	1
9) İşe alınan ve ayrılan personel – güvenlik hususları	2
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	4
11) Kurum dışı kişiler- fiziksel güvenlik	3
12) Ekipman ve techizat güvenliği	3
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	3
14) Zararlı yazılımlara karşı güvenlik	3
15) Bilgi iletişim ortamları güvenliği	4
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	4
17) Ağ erişimi güvenliği	4
18) Bilgi sistemleri geliştirilmesi ve bakımı	2
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	3
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	3
21) İş sürekliliği yönetimi	3
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	2
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	2
24) Bilgi güvenliği yönetimi izleme ve denetimi	2
Toplam	**61**
Ortalama Değer	**2.54**

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	61.00 / 120.00 puan	118.08 / 120.00 puan	88.32 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	2.54	4.92	3.68

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : Ortalamadan Düşük Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Yüksek Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ortalama düzeyin altındadır.
Buna göre aşağıdakiler önerilmektedir:

- Öncelikle kurum için bilgi güvenliği farkındalığı bilgilenme eğitim ve/veya çalıştayı gerçekleştirilmesi çok önemlidir. Bu eğitimin öncelikle yönetimi ve ilgili kişileri kapsaması ve daha sonra kurum geneline yaygınlaştırılması uygundur. Bu çalıştayların kurum içinde periyodik olarak ve interaktif yöntemlerle yapılması; çalışanların bilincinin aktif ve sürekli tutulması ve bilgi güvenliğinin günlük iş ortamındaki davranışlara yansıtılması açısından özellikle önerilmektedir.
- Kurumun bilgi güvenliği ihtiyaçlarına hizmet verebilecek şekilde bilgi güvenliği yönetimi sistematiklerinin oluşturulması, varsa tekrar gözden geçirilerek iyileştirilmesi. Bunu yaparken, uluslararası standartları (örneğin; ISO/IEC 27001 veya kurumun yasal olarak uyması gerekli benzeri standartları) dikkate almak yol gösterici olacaktır.
- Grubunuzdaki ortalama seviyeye ulaşmanın hedeflenmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	Ortalamadan Düşük Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	Ortalamadan Düşük Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	Ortalamadan Düşük Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	Ortalamadan Düşük Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	Ortalamadan Düşük Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	Ortalamadan Düşük Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	Ortalamadan Düşük Seviyede
2	Organizasyonel yapılanma	Ortalamadan Düşük Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	Ortalamadan Düşük Seviyede
4	Bilgi varlıklarının korunması	Ortalamadan Düşük Seviyede
5	Bilgi varlıkları sınıflandırması	Ortalamadan Düşük Seviyede
6	Bilgi varlıkları risk değerlendirme	Ortalamadan Düşük Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	Ortalamadan Düşük Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	Ortalamadan Düşük Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	Ortalamadan Düşük Seviyede
10	Fiziksel güvenlik	Ortalamadan Düşük Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	Ortalamadan Düşük Seviyede
12	Ekipman ve techizat güvenliği	Ortalamadan Düşük Seviyede
13	Operasyonel bilgi sistemi güvenliği	Ortalama Seviyede
14	Zararlı yazılımlara karşı güvenlik	Ortalamadan Düşük Seviyede
15	Bilgi iletişim ortamları güvenliği	Ortalama Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	Ortalamadan Düşük Seviyede
17	Ağ erişimi güvenliği	Ortalamadan Düşük Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	Ortalamadan Düşük Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	Ortalamadan Düşük Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	Ortalamadan Düşük Seviyede
21	İş sürekliliği yönetimi	Ortalamadan Düşük Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	Ortalamadan Düşük Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	Ortalamadan Düşük Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	Ortalamadan Düşük Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli
Kurum Adı : KURUM 14
Faaliyet Alanı : K-FİNANS VE SİGORTA FAALİYETLERİ
Kurum Ölçeği : Büyük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

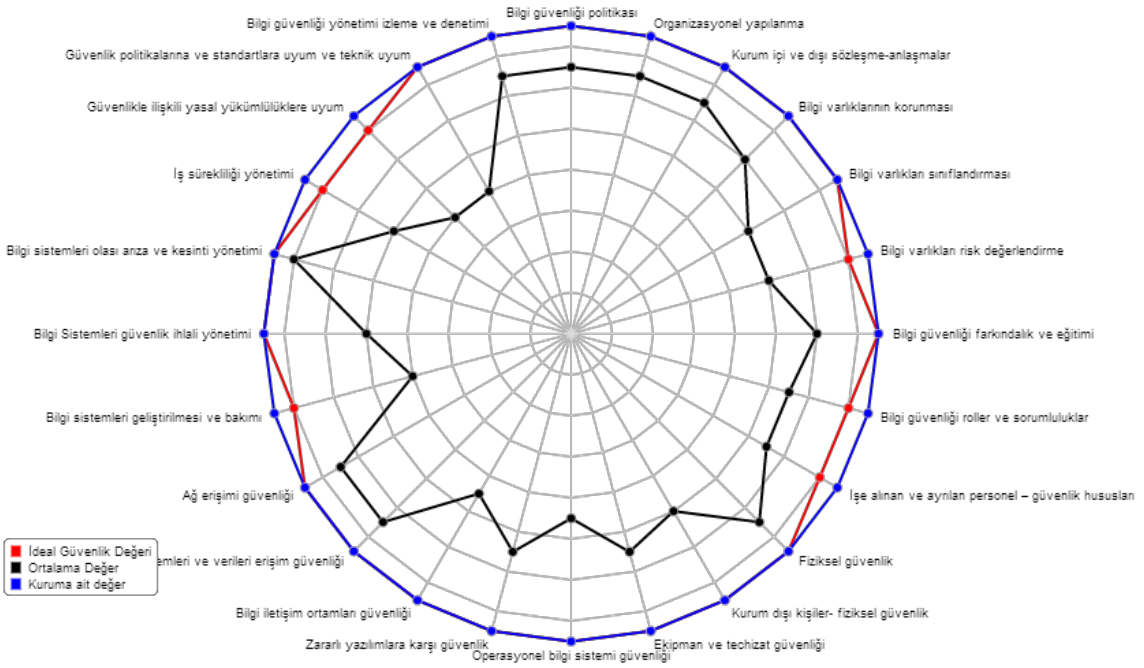
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	5
2) Organizasyonel yapılanma	5
3) Kurum içi ve dışı sözleşme-anlaşmalar	5
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	5
5) Bilgi varlıkları sınıflandırması	5
6) Bilgi varlıkları risk değerlendirme	5
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	5
8) Bilgi güvenliği roller ve sorumluluklar	5
9) İşe alınan ve ayrılan personel – güvenlik hususları	5
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	5
11) Kurum dışı kişiler- fiziksel güvenlik	5
12) Ekipman ve techizat güvenliği	5
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	5
14) Zararlı yazılımlara karşı güvenlik	5
15) Bilgi iletişim ortamları güvenliği	5
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	5
17) Ağ erişimi güvenliği	5
18) Bilgi sistemleri geliştirilmesi ve bakımı	5
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	5
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	5
21) İş sürekliliği yönetimi	5
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	5
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	5
24) Bilgi güvenliği yönetimi izleme ve denetimi	5
Toplam	**120**
Ortalama Değer	**5.00**

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	120.00 / 120.00 puan	118.08 / 120.00 puan	88.32 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	5.00	4.92	3.68

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : İdeal Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Yüksek Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ideal düzeydedir. Tebrikler !
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyenin korunması için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştayların sürdürülmesi.
- İdeal seviyenin korunması için gerekli gözden geçirme ve iyileştirme döngüsünün sürdürülmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	İdeal Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	İdeal Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	İdeal Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	İdeal Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	İdeal Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	İdeal Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	İdeal Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	İdeal Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	İdeal Seviyede
2	Organizasyonel yapılanma	İdeal Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	İdeal Seviyede
4	Bilgi varlıklarının korunması	İdeal Seviyede
5	Bilgi varlıkları sınıflandırması	İdeal Seviyede
6	Bilgi varlıkları risk değerlendirme	İdeal Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	İdeal Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	İdeal Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	İdeal Seviyede
10	Fiziksel güvenlik	İdeal Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	İdeal Seviyede
12	Ekipman ve techizat güvenliği	İdeal Seviyede
13	Operasyonel bilgi sistemi güvenliği	İdeal Seviyede
14	Zararlı yazılımlara karşı güvenlik	İdeal Seviyede
15	Bilgi iletişim ortamları güvenliği	İdeal Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	İdeal Seviyede
17	Ağ erişimi güvenliği	İdeal Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	İdeal Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	İdeal Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	İdeal Seviyede
21	İş sürekliliği yönetimi	İdeal Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	İdeal Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	İdeal Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	İdeal Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli
Kurum Adı : KURUM 15
Faaliyet Alanı : M: MESLEKİ, BİLİMSEL VE TEKNİK FAALİYETLER
Kurum Ölçeği : Küçük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

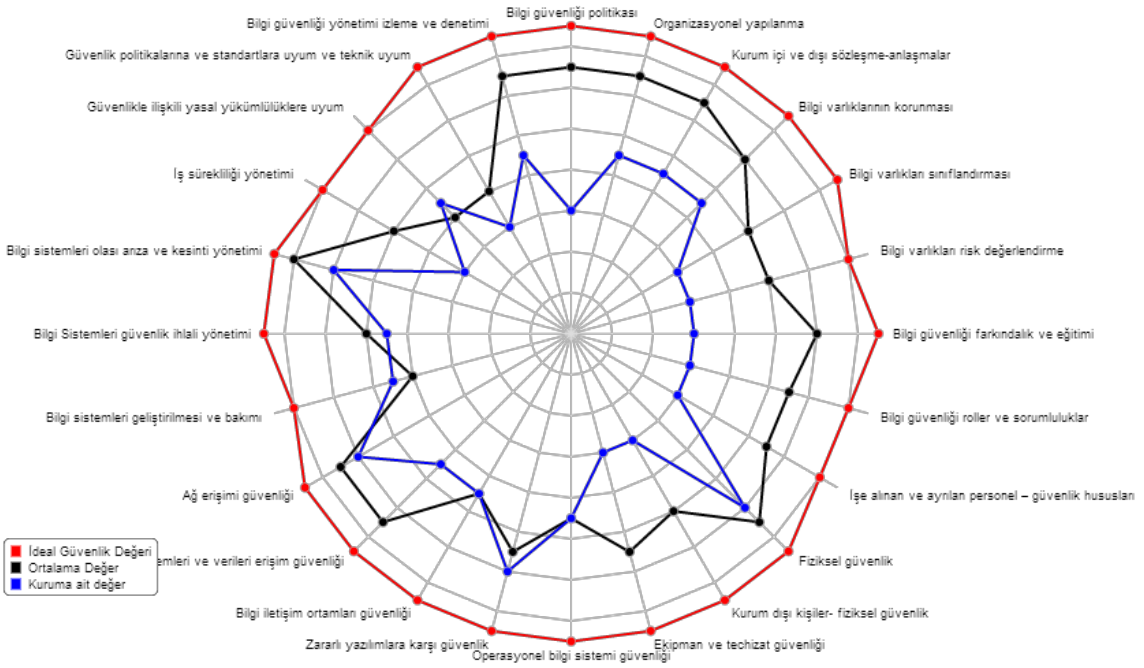
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	2
2) Organizasyonel yapılanma	3
3) Kurum içi ve dışı sözleşme-anlaşmalar	3
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	3
5) Bilgi varlıkları sınıflandırması	2
6) Bilgi varlıkları risk değerlendirme	2
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	2
8) Bilgi güvenliği roller ve sorumluluklar	2
9) İşe alınan ve ayrılan personel – güvenlik hususları	2
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	4
11) Kurum dışı kişiler- fiziksel güvenlik	2
12) Ekipman ve techizat güvenliği	2
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	3
14) Zararlı yazılımlara karşı güvenlik	4
15) Bilgi iletişim ortamları güvenliği	3
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	3
17) Ağ erişimi güvenliği	4
18) Bilgi sistemleri geliştirilmesi ve bakımı	3
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	3
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	4
21) İş sürekliliği yönetimi	2
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	3
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	2
24) Bilgi güvenliği yönetimi izleme ve denetimi	3
Toplam	**66**
Ortalama Değer	**2.75**

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	66.00 / 120.00 puan	118.08 / 120.00 puan	88.32 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	2.75	4.92	3.68

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : Ortalamadan Düşük Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Yüksek Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ortalama düzeyin altındadır.
Buna göre aşağıdakiler önerilmektedir:

- Öncelikle kurum için bilgi güvenliği farkındalığı bilgilenme eğitim ve/veya çalıştayı gerçekleştirilmesi çok önemlidir. Bu eğitimin öncelikle yönetimi ve ilgili kişileri kapsaması ve daha sonra kurum geneline yaygınlaştırılması uygundur. Bu çalıştayların kurum içinde periyodik olarak ve interaktif yöntemlerle yapılması; çalışanların bilincinin aktif ve sürekli tutulması ve bilgi güvenliğinin günlük iş ortamındaki davranışlara yansıtılması açısından özellikle önerilmektedir.
- Kurumun bilgi güvenliği ihtiyaçlarına hizmet verebilecek şekilde bilgi güvenliği yönetimi sistematiklerinin oluşturulması, varsa tekrar gözden geçirilerek iyileştirilmesi. Bunu yaparken, uluslararası standartları (örneğin; ISO/IEC 27001 veya kurumun yasal olarak uyması gerekli benzeri standartları) dikkate almak yol gösterici olacaktır.
- Grubunuzdaki ortalama seviyeye ulaşmanın hedeflenmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	Ortalamadan Düşük Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	Ortalamadan Düşük Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	Ortalamadan Düşük Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	Ortalamadan Düşük Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	Ortalamadan Düşük Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	Ortalamadan Düşük Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	Ortalamadan Düşük Seviyede
2	Organizasyonel yapılanma	Ortalamadan Düşük Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	Ortalamadan Düşük Seviyede
4	Bilgi varlıklarının korunması	Ortalamadan Düşük Seviyede
5	Bilgi varlıkları sınıflandırması	Ortalamadan Düşük Seviyede
6	Bilgi varlıkları risk değerlendirme	Ortalamadan Düşük Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	Ortalamadan Düşük Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	Ortalamadan Düşük Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	Ortalamadan Düşük Seviyede
10	Fiziksel güvenlik	Ortalamadan Düşük Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	Ortalamadan Düşük Seviyede
12	Ekipman ve techizat güvenliği	Ortalamadan Düşük Seviyede
13	Operasyonel bilgi sistemi güvenliği	Ortalama Seviyede
14	Zararlı yazılımlara karşı güvenlik	Ortalama Seviyede
15	Bilgi iletişim ortamları güvenliği	Ortalama Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	Ortalamadan Düşük Seviyede
17	Ağ erişimi güvenliği	Ortalamadan Düşük Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	Ortalama Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	Ortalamadan Düşük Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	Ortalamadan Düşük Seviyede
21	İş sürekliliği yönetimi	Ortalamadan Düşük Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	Ortalama Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	Ortalamadan Düşük Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	Ortalamadan Düşük Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri ORTA DÜZEYDE gerekli
Kurum Adı : KURUM 16
Faaliyet Alanı : M-MESLEKİ, BİLİMSEL VE TEKNİK FAALİYETLER
Kurum Ölçeği : Küçük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

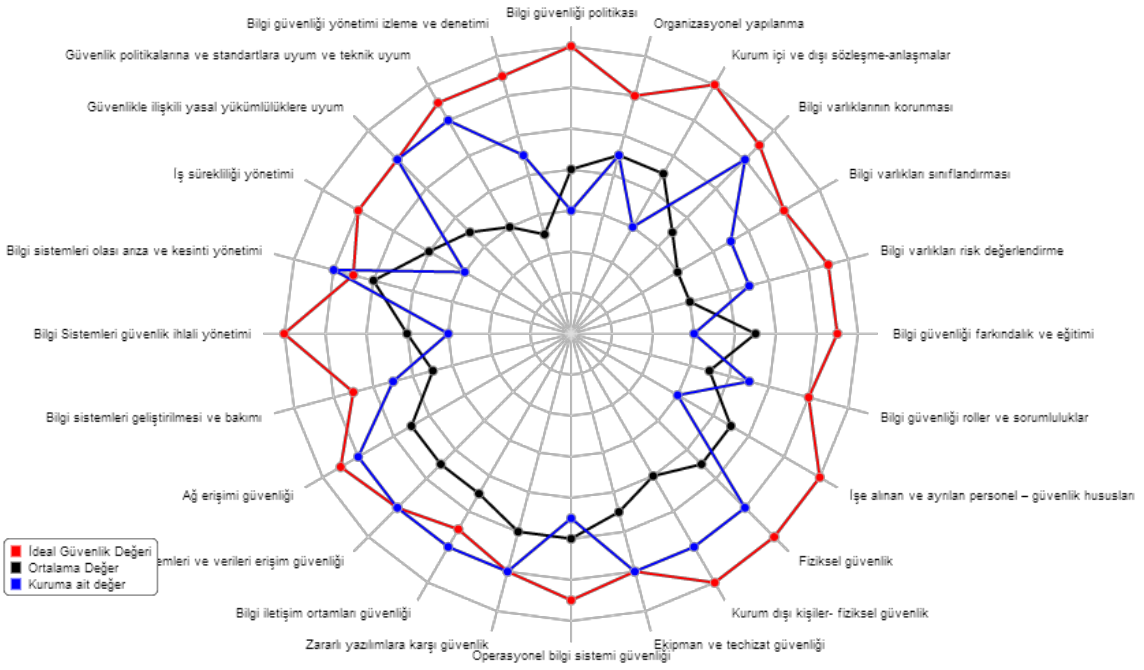
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	2
2) Organizasyonel yapılanma	3
3) Kurum içi ve dışı sözleşme-anlaşmalar	2
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	4
5) Bilgi varlıkları sınıflandırması	3
6) Bilgi varlıkları risk değerlendirme	3
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	2
8) Bilgi güvenliği roller ve sorumluluklar	3
9) İşe alınan ve ayrılan personel – güvenlik hususları	2
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	4
11) Kurum dışı kişiler- fiziksel güvenlik	4
12) Ekipman ve techizat güvenliği	4
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	3
14) Zararlı yazılımlara karşı güvenlik	4
15) Bilgi iletişim ortamları güvenliği	4
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	4
17) Ağ erişimi güvenliği	4
18) Bilgi sistemleri geliştirilmesi ve bakımı	3
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	2
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	4
21) İş sürekliliği yönetimi	2
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	4
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	4
24) Bilgi güvenliği yönetimi izleme ve denetimi	3
Toplam	**77**
Ortalama Değer	**3.21**

Seçilen Grup : Bilgi Güvenliği tedbirleri ORTA DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	77.00 / 120.00 puan	101.28 / 120.00 puan	64.56 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	3.21	4.22	2.69

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : Ortalama Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Orta Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ortalama düzeydedir.
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyeyi korumak ve iyileştirmek için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştaylar yapılması.
- Radar grafiği ve değerlendirme sonuçlarına göre; iyileştirilmesi gerekli hususların belirlenmesi, gözden geçirme ve iyileştirme çalışmaları yapılması. Bunu yaparken, uluslararası standartları (örneğin; ISO/IEC 27001 veya kurumun yasal olarak uyması gerekli benzeri standartları) dikkate almak yol gösterici olacaktır.
- Grubunuzdaki ideal seviyeye ulaşmanın hedeflenmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	Ortalamadan Düşük Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	Ortalama Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	Ortalama Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	Ortalama Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	Ortalama Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	Ortalamadan Düşük Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	Ortalama Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	Ortalamadan Düşük Seviyede
2	Organizasyonel yapılanma	Ortalama Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	Ortalamadan Düşük Seviyede
4	Bilgi varlıklarının korunması	Ortalama Seviyede
5	Bilgi varlıkları sınıflandırması	Ortalama Seviyede
6	Bilgi varlıkları risk değerlendirme	Ortalama Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	Ortalamadan Düşük Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	Ortalama Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	Ortalamadan Düşük Seviyede
10	Fiziksel güvenlik	Ortalama Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	Ortalama Seviyede
12	Ekipman ve techizat güvenliği	İdeal Seviyede
13	Operasyonel bilgi sistemi güvenliği	Ortalamadan Düşük Seviyede
14	Zararlı yazılımlara karşı güvenlik	İdeal Seviyede
15	Bilgi iletişim ortamları güvenliği	İdeal Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	İdeal Seviyede
17	Ağ erişimi güvenliği	Ortalama Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	Ortalama Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	Ortalamadan Düşük Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	İdeal Seviyede
21	İş sürekliliği yönetimi	Ortalamadan Düşük Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	İdeal Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	Ortalama Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	Ortalama Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri DÜŞÜK DÜZEYDE gerekli
Kurum Adı : KURUM 17
Faaliyet Alanı : J-BİLGİ VE İLETİŞİM
Kurum Ölçeği : Küçük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

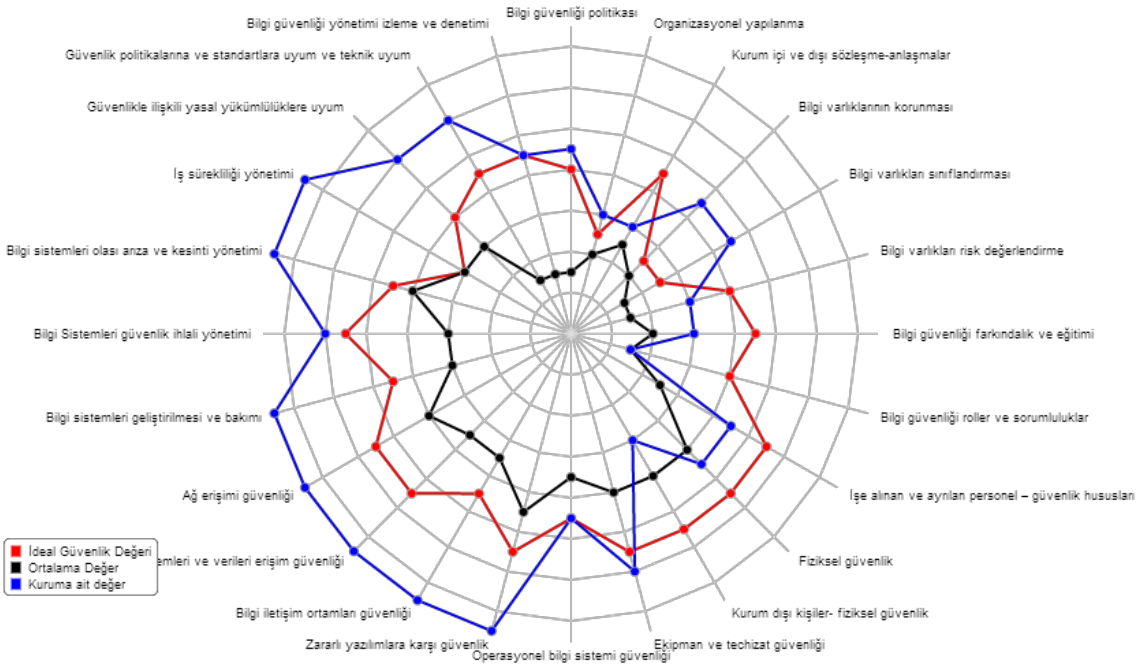
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	3
2) Organizasyonel yapılanma	2
3) Kurum içi ve dışı sözleşme-anlaşmalar	2
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	3
5) Bilgi varlıkları sınıflandırması	3
6) Bilgi varlıkları risk değerlendirme	2
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	2
8) Bilgi güvenliği roller ve sorumluluklar	1
9) İşe alınan ve ayrılan personel – güvenlik hususları	3
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	3
11) Kurum dışı kişiler- fiziksel güvenlik	2
12) Ekipman ve techizat güvenliği	4
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	3
14) Zararlı yazılımlara karşı güvenlik	5
15) Bilgi iletişim ortamları güvenliği	5
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	5
17) Ağ erişimi güvenliği	5
18) Bilgi sistemleri geliştirilmesi ve bakımı	5
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	4
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	5
21) İş sürekliliği yönetimi	5
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	4
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	4
24) Bilgi güvenliği yönetimi izleme ve denetimi	3
Toplam	**83**
Ortalama Değer	**3.46**

Seçilen Grup : Bilgi Güvenliği tedbirleri DÜŞÜK DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	83.00 / 120.00 puan	71.04 / 120.00 puan	44.64 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	3.46	2.96	1.86

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : İdeal Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Düşük Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ideal düzeydedir. Tebrikler !
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyenin korunması için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştayların sürdürülmesi.
- İdeal seviyenin korunması için gerekli gözden geçirme ve iyileştirme döngüsünün sürdürülmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	Ortalama Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	Ortalama Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	Ortalama Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	İdeal Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	İdeal Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	İdeal Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	İdeal Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	İdeal Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	İdeal Seviyede
2	Organizasyonel yapılanma	İdeal Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	Ortalama Seviyede
4	Bilgi varlıklarının korunması	İdeal Seviyede
5	Bilgi varlıkları sınıflandırması	İdeal Seviyede
6	Bilgi varlıkları risk değerlendirme	Ortalama Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	Ortalama Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	Ortalama Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	Ortalama Seviyede
10	Fiziksel güvenlik	Ortalama Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	Ortalamadan Düşük Seviyede
12	Ekipman ve techizat güvenliği	İdeal Seviyede
13	Operasyonel bilgi sistemi güvenliği	İdeal Seviyede
14	Zararlı yazılımlara karşı güvenlik	İdeal Seviyede
15	Bilgi iletişim ortamları güvenliği	İdeal Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	İdeal Seviyede
17	Ağ erişimi güvenliği	İdeal Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	İdeal Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	İdeal Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	İdeal Seviyede
21	İş sürekliliği yönetimi	İdeal Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	İdeal Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	İdeal Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	İdeal Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri DÜŞÜK DÜZEYDE gerekli
Kurum Adı : KURUM 18
Faaliyet Alanı : J-BİLGİ VE İLETİŞİM
Kurum Ölçeği : Küçük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

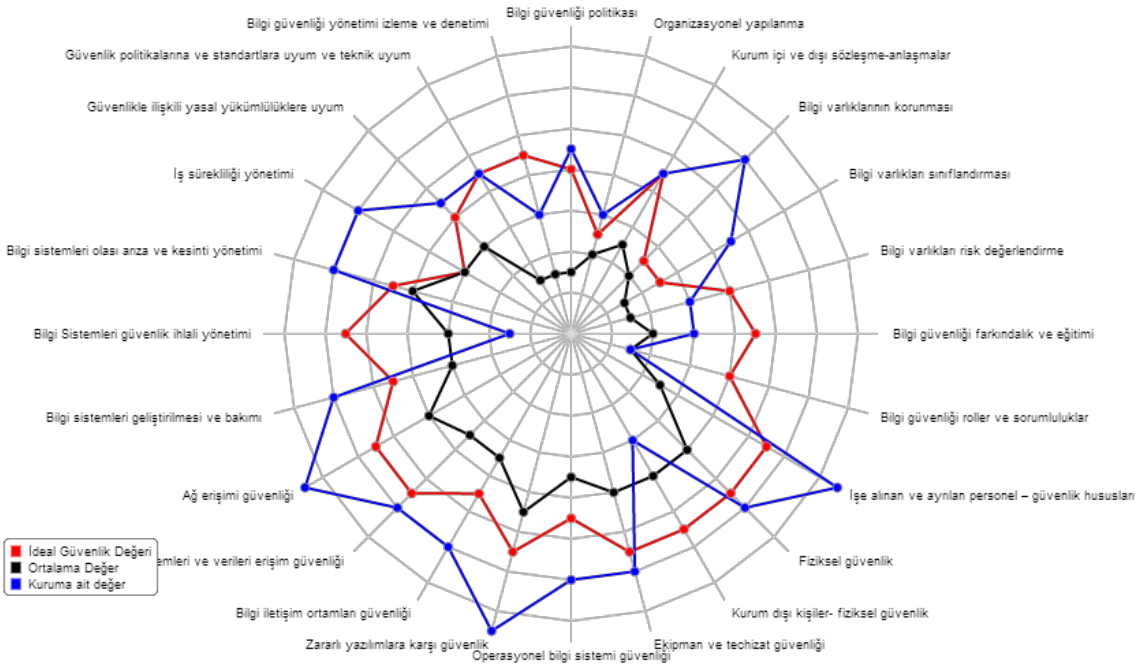
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	3
2) Organizasyonel yapılanma	2
3) Kurum içi ve dışı sözleşme-anlaşmalar	3
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	4
5) Bilgi varlıkları sınıflandırması	3
6) Bilgi varlıkları risk değerlendirme	2
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	2
8) Bilgi güvenliği roller ve sorumluluklar	1
9) İşe alınan ve ayrılan personel – güvenlik hususları	5
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	4
11) Kurum dışı kişiler- fiziksel güvenlik	2
12) Ekipman ve techizat güvenliği	4
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	4
14) Zararlı yazılımlara karşı güvenlik	5
15) Bilgi iletişim ortamları güvenliği	4
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	4
17) Ağ erişimi güvenliği	5
18) Bilgi sistemleri geliştirilmesi ve bakımı	4
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	1
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	4
21) İş sürekliliği yönetimi	4
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	3
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	3
24) Bilgi güvenliği yönetimi izleme ve denetimi	2
Toplam	**78**
Ortalama Değer	**3.25**

Seçilen Grup : Bilgi Güvenliği tedbirleri DÜŞÜK DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	78.00 / 120.00 puan	71.04 / 120.00 puan	44.64 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	3.25	2.96	1.86

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : İdeal Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Düşük Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ideal düzeydedir. Tebrikler !
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyenin korunması için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştayların sürdürülmesi.
- İdeal seviyenin korunması için gerekli gözden geçirme ve iyileştirme döngüsünün sürdürülmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	Ortalama Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	İdeal Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	Ortalama Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	İdeal Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	İdeal Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	İdeal Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	İdeal Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	Ortalama Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	İdeal Seviyede
2	Organizasyonel yapılanma	İdeal Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	İdeal Seviyede
4	Bilgi varlıklarının korunması	İdeal Seviyede
5	Bilgi varlıkları sınıflandırması	İdeal Seviyede
6	Bilgi varlıkları risk değerlendirme	Ortalama Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	Ortalama Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	Ortalama Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	İdeal Seviyede
10	Fiziksel güvenlik	İdeal Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	Ortalamadan Düşük Seviyede
12	Ekipman ve techizat güvenliği	İdeal Seviyede
13	Operasyonel bilgi sistemi güvenliği	İdeal Seviyede
14	Zararlı yazılımlara karşı güvenlik	İdeal Seviyede
15	Bilgi iletişim ortamları güvenliği	İdeal Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	İdeal Seviyede
17	Ağ erişimi güvenliği	İdeal Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	İdeal Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	Ortalamadan Düşük Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	İdeal Seviyede
21	İş sürekliliği yönetimi	İdeal Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	İdeal Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	İdeal Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	Ortalama Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli
Kurum Adı : KURUM 19
Faaliyet Alanı : J-BİLGİ VE İLETİŞİM
Kurum Ölçeği : Küçük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

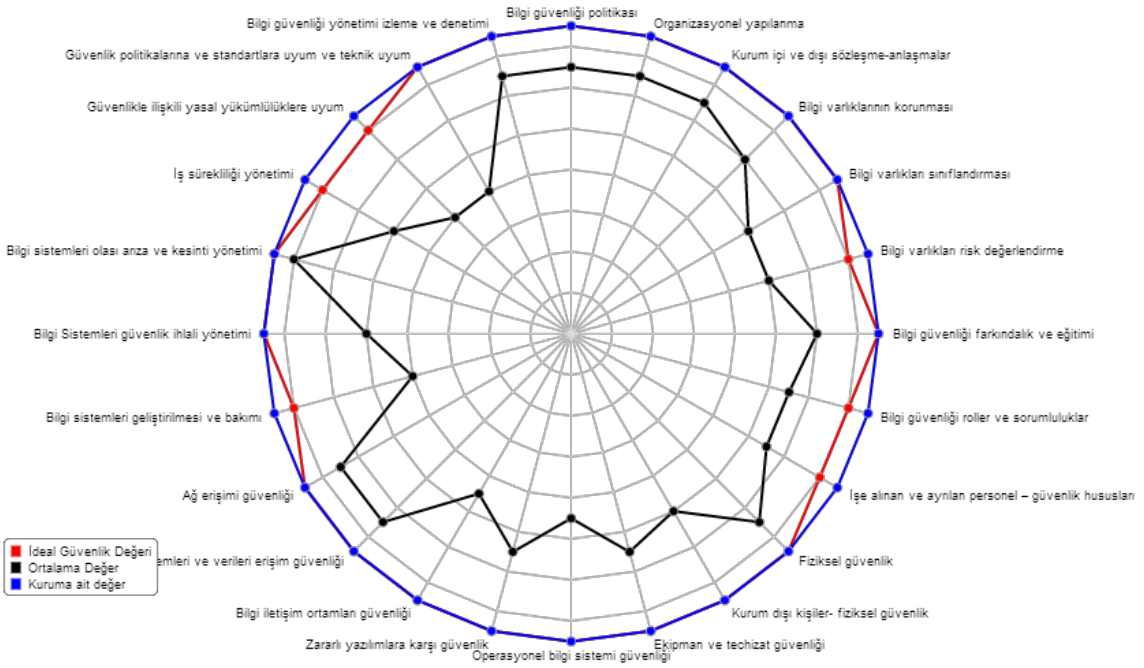
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	5
2) Organizasyonel yapılanma	5
3) Kurum içi ve dışı sözleşme-anlaşmalar	5
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	5
5) Bilgi varlıkları sınıflandırması	5
6) Bilgi varlıkları risk değerlendirme	5
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	5
8) Bilgi güvenliği roller ve sorumluluklar	5
9) İşe alınan ve ayrılan personel – güvenlik hususları	5
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	5
11) Kurum dışı kişiler- fiziksel güvenlik	5
12) Ekipman ve techizat güvenliği	5
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	5
14) Zararlı yazılımlara karşı güvenlik	5
15) Bilgi iletişim ortamları güvenliği	5
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	5
17) Ağ erişimi güvenliği	5
18) Bilgi sistemleri geliştirilmesi ve bakımı	5
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	5
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	5
21) İş sürekliliği yönetimi	5
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	5
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	5
24) Bilgi güvenliği yönetimi izleme ve denetimi	5
Toplam	**120**
Ortalama Değer	**5.00**

Seçilen Grup : Bilgi Güvenliği tedbirleri YÜKSEK DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	120.00 / 120.00 puan	118.08 / 120.00 puan	88.32 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	5.00	4.92	3.68

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : İdeal Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Yüksek Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ideal düzeydedir. Tebrikler !
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyenin korunması için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştayların sürdürülmesi.
- İdeal seviyenin korunması için gerekli gözden geçirme ve iyileştirme döngüsünün sürdürülmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	İdeal Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	İdeal Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	İdeal Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	İdeal Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	İdeal Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	İdeal Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	İdeal Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	İdeal Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	İdeal Seviyede
2	Organizasyonel yapılanma	İdeal Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	İdeal Seviyede
4	Bilgi varlıklarının korunması	İdeal Seviyede
5	Bilgi varlıkları sınıflandırması	İdeal Seviyede
6	Bilgi varlıkları risk değerlendirme	İdeal Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	İdeal Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	İdeal Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	İdeal Seviyede
10	Fiziksel güvenlik	İdeal Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	İdeal Seviyede
12	Ekipman ve techizat güvenliği	İdeal Seviyede
13	Operasyonel bilgi sistemi güvenliği	İdeal Seviyede
14	Zararlı yazılımlara karşı güvenlik	İdeal Seviyede
15	Bilgi iletişim ortamları güvenliği	İdeal Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	İdeal Seviyede
17	Ağ erişimi güvenliği	İdeal Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	İdeal Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	İdeal Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	İdeal Seviyede
21	İş sürekliliği yönetimi	İdeal Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	İdeal Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	İdeal Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	İdeal Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri ORTA DÜZEYDE gerekli
Kurum Adı : KURUM 20
Faaliyet Alanı : P-EĞİTİM
Kurum Ölçeği : Orta Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

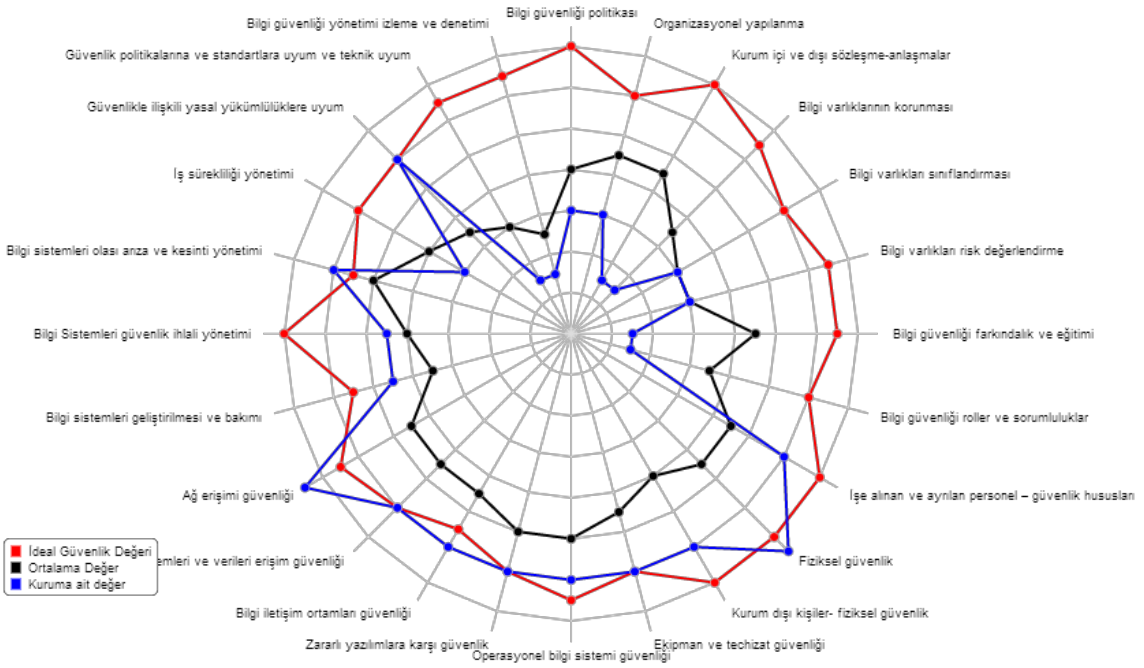
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	2
2) Organizasyonel yapılanma	2
3) Kurum içi ve dışı sözleşme-anlaşmalar	1
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	1
5) Bilgi varlıkları sınıflandırması	2
6) Bilgi varlıkları risk değerlendirme	2
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	1
8) Bilgi güvenliği roller ve sorumluluklar	1
9) İşe alınan ve ayrılan personel – güvenlik hususları	4
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	5
11) Kurum dışı kişiler- fiziksel güvenlik	4
12) Ekipman ve techizat güvenliği	4
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	4
14) Zararlı yazılımlara karşı güvenlik	4
15) Bilgi iletişim ortamları güvenliği	4
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	4
17) Ağ erişimi güvenliği	5
18) Bilgi sistemleri geliştirilmesi ve bakımı	3
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	3
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	4
21) İş sürekliliği yönetimi	2
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	4
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	1
24) Bilgi güvenliği yönetimi izleme ve denetimi	1
Toplam	**68**
Ortalama Değer	**2.83**

Seçilen Grup : Bilgi Güvenliği tedbirleri ORTA DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	68.00 / 120.00 puan	101.28 / 120.00 puan	64.56 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	2.83	4.22	2.69

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : Ortalama Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Orta Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ortalama düzeydedir.
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyeyi korumak ve iyileştirmek için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştaylar yapılması.
- Radar grafiği ve değerlendirme sonuçlarına göre; iyileştirilmesi gerekli hususların belirlenmesi, gözden geçirme ve iyileştirme çalışmaları yapılması. Bunu yaparken, uluslararası standartları (örneğin; ISO/IEC 27001 veya kurumun yasal olarak uyması gerekli benzeri standartları) dikkate almak yol gösterici olacaktır.
- Grubunuzdaki ideal seviyeye ulaşmanın hedeflenmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	Ortalamadan Düşük Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	Ortalama Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	Ortalama Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	Ortalama Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	Ortalama Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	Ortalamadan Düşük Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	Ortalamadan Düşük Seviyede
2	Organizasyonel yapılanma	Ortalamadan Düşük Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	Ortalamadan Düşük Seviyede
4	Bilgi varlıklarının korunması	Ortalamadan Düşük Seviyede
5	Bilgi varlıkları sınıflandırması	Ortalama Seviyede
6	Bilgi varlıkları risk değerlendirme	Ortalama Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	Ortalamadan Düşük Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	Ortalamadan Düşük Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	Ortalama Seviyede
10	Fiziksel güvenlik	İdeal Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	Ortalama Seviyede
12	Ekipman ve techizat güvenliği	İdeal Seviyede
13	Operasyonel bilgi sistemi güvenliği	Ortalama Seviyede
14	Zararlı yazılımlara karşı güvenlik	İdeal Seviyede
15	Bilgi iletişim ortamları güvenliği	İdeal Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	İdeal Seviyede
17	Ağ erişimi güvenliği	İdeal Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	Ortalama Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	Ortalama Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	İdeal Seviyede
21	İş sürekliliği yönetimi	Ortalamadan Düşük Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	İdeal Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	Ortalamadan Düşük Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	Ortalamadan Düşük Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri ORTA DÜZEYDE gerekli
Kurum Adı : KURUM 21
Faaliyet Alanı : P-EĞİTİM
Kurum Ölçeği : Küçük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

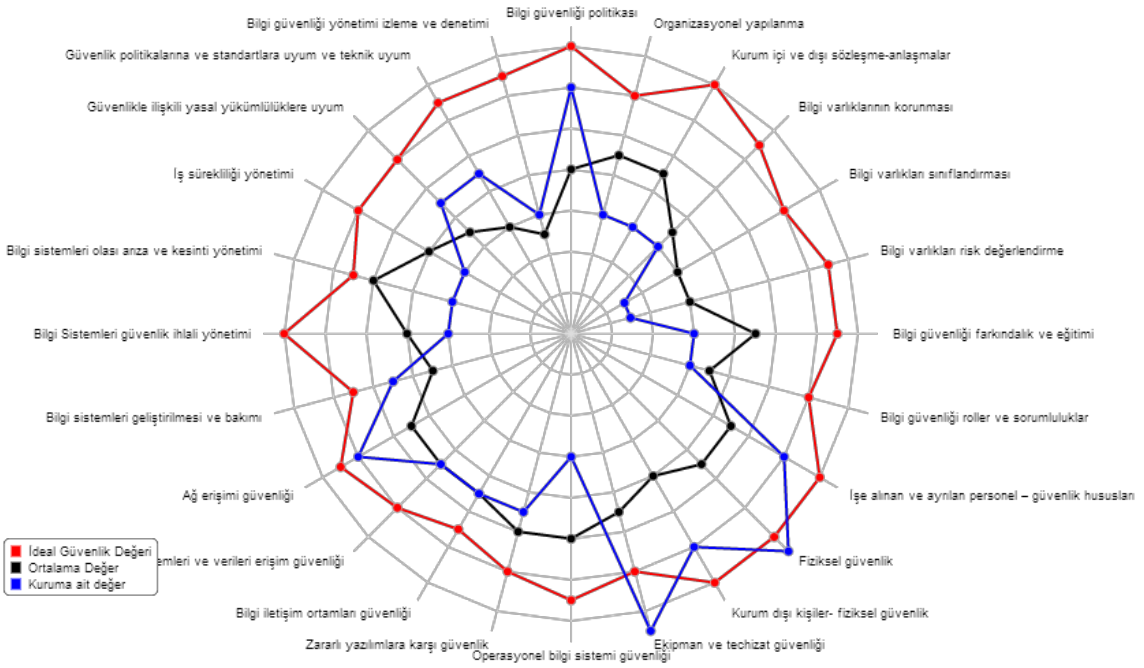
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	4
2) Organizasyonel yapılanma	2
3) Kurum içi ve dışı sözleşme-anlaşmalar	2
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	2
5) Bilgi varlıkları sınıflandırması	1
6) Bilgi varlıkları risk değerlendirme	1
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	2
8) Bilgi güvenliği roller ve sorumluluklar	2
9) İşe alınan ve ayrılan personel – güvenlik hususları	4
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	5
11) Kurum dışı kişiler- fiziksel güvenlik	4
12) Ekipman ve techizat güvenliği	5
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	2
14) Zararlı yazılımlara karşı güvenlik	3
15) Bilgi iletişim ortamları güvenliği	3
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	3
17) Ağ erişimi güvenliği	4
18) Bilgi sistemleri geliştirilmesi ve bakımı	3
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	2
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	2
21) İş sürekliliği yönetimi	2
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	3
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	3
24) Bilgi güvenliği yönetimi izleme ve denetimi	2
Toplam	**66**
Ortalama Değer	**2.75**

Seçilen Grup : Bilgi Güvenliği tedbirleri ORTA DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	66.00 / 120.00 puan	101.28 / 120.00 puan	64.56 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	2.75	4.22	2.69

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : Ortalama Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Orta Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ortalama düzeydedir.
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyeyi korumak ve iyileştirmek için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştaylar yapılması.
- Radar grafiği ve değerlendirme sonuçlarına göre; iyileştirilmesi gerekli hususların belirlenmesi, gözden geçirme ve iyileştirme çalışmaları yapılması. Bunu yaparken, uluslararası standartları (örneğin; ISO/IEC 27001 veya kurumun yasal olarak uyması gerekli benzeri standartları) dikkate almak yol gösterici olacaktır.
- Grubunuzdaki ideal seviyeye ulaşmanın hedeflenmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	Ortalamadan Düşük Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	Ortalama Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	Ortalamadan Düşük Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	Ortalama Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	Ortalamadan Düşük Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	Ortalamadan Düşük Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	Ortalama Seviyede
2	Organizasyonel yapılanma	Ortalamadan Düşük Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	Ortalamadan Düşük Seviyede
4	Bilgi varlıklarının korunması	Ortalamadan Düşük Seviyede
5	Bilgi varlıkları sınıflandırması	Ortalamadan Düşük Seviyede
6	Bilgi varlıkları risk değerlendirme	Ortalamadan Düşük Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	Ortalamadan Düşük Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	Ortalamadan Düşük Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	Ortalama Seviyede
10	Fiziksel güvenlik	İdeal Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	Ortalama Seviyede
12	Ekipman ve techizat güvenliği	İdeal Seviyede
13	Operasyonel bilgi sistemi güvenliği	Ortalamadan Düşük Seviyede
14	Zararlı yazılımlara karşı güvenlik	Ortalamadan Düşük Seviyede
15	Bilgi iletişim ortamları güvenliği	Ortalama Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	Ortalama Seviyede
17	Ağ erişimi güvenliği	Ortalama Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	Ortalama Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	Ortalamadan Düşük Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	Ortalamadan Düşük Seviyede
21	İş sürekliliği yönetimi	Ortalamadan Düşük Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	Ortalama Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	Ortalama Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	Ortalama Seviyede

Bilgi Güvenliği Yönetimi Değerlendirme Sonuçları

Seçilen Grup : Bilgi Güvenliği tedbirleri ORTA DÜZEYDE gerekli
Kurum Adı : KURUM 23
Faaliyet Alanı : J-BİLGİ VE İLETİŞİM
Kurum Ölçeği : Küçük Ölçekli

Değerlendirme Puanlaması

1 -	Uygulanmamaktadır	Yönetimin gerekliliği konusunda farkındalığı yoktur, bu konuda kurumsal bilinçlendirilmeye gerek vardır.
2 -	Farkındalık mevcut ancak uygulanmamaktadır	Yönetim tarafından gerekliliği bilinmekte, uygulanması planlanmaktadır, herhangi bir politika ve kural oluşturulmamıştır.
3 -	Kısmen uygulanmaktadır	Nadiren veya kısıtlı seviyede kural ve kontrol uygulanmaktadır. Politika ve kurallar yazılı değil veya kısmen yazılıdır.
4 -	Uygulanmakta ancak periyodik gözden geçirme yapılmamaktadır	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta ancak gözden geçirme ve izleme yapılmamaktadır.
5 -	Uygulanmakta, denetlenmekte ve kurum ihtiyaçlarına göre iyileştirilmektedir	Kontroller, kurallar yazılı ve organizasyon genelinde uygulanmakta periyodik denetlenmekte, gözden geçirilmekte ve iyileştirilmektedir

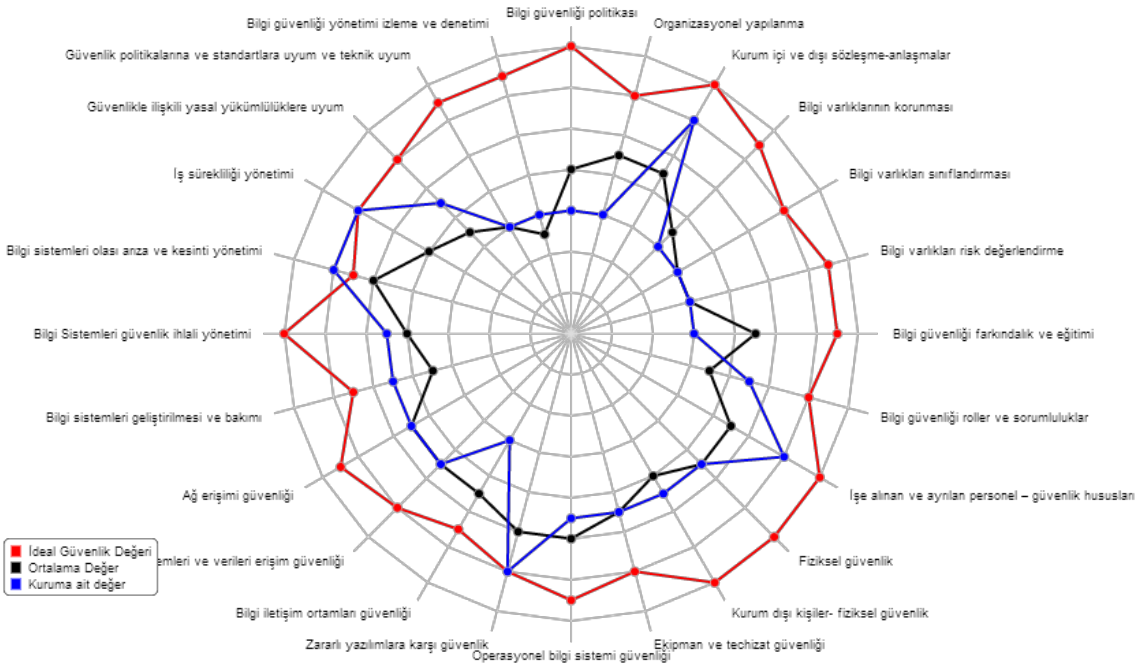
(Puan, cevap anahtarından seçilen cevaba göre 1 ile 5 arasında verilir. 1 en düşük, 5 en yüksek puandır)

Soru	Puan
Bölüm 1-Bilgi Güvenliğine Kurumsal Yaklaşım	
1) Bilgi güvenliği politikası	2
2) Organizasyonel yapılanma	2
3) Kurum içi ve dışı sözleşme-anlaşmalar	4
Bölüm 2-Bilgi Varlıkları Güvenliği Yönetimi	
4) Bilgi varlıklarının korunması	2
5) Bilgi varlıkları sınıflandırması	2
6) Bilgi varlıkları risk değerlendirme	2
Bölüm 3-İnsan Kaynakları Güvenliği Yönetimi	
7) Bilgi güvenliği farkındalık ve eğitimi	2
8) Bilgi güvenliği roller ve sorumluluklar	3
9) İşe alınan ve ayrılan personel – güvenlik hususları	4
Bölüm 4-Fiziksel ve Çevresel Güvenlik Yönetimi	
10) Fiziksel güvenlik	3
11) Kurum dışı kişiler- fiziksel güvenlik	3
12) Ekipman ve techizat güvenliği	3
Bölüm 5-Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	
13) Operasyonel bilgi sistemi güvenliği	3
14) Zararlı yazılımlara karşı güvenlik	4
15) Bilgi iletişim ortamları güvenliği	2
Bölüm 6-Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	
16) Bilgi sistemleri ve verileri erişim güvenliği	3
17) Ağ erişimi güvenliği	3
18) Bilgi sistemleri geliştirilmesi ve bakımı	3
Bölüm 7-Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	
19) Bilgi Sistemleri güvenlik ihlali yönetimi	3
20) Bilgi sistemleri olası arıza ve kesinti yönetimi	4
21) İş sürekliliği yönetimi	4
Bölüm 8-Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	
22) Güvenlikle ilişkili yasal yükümlülüklere uyum	3
23) Güvenlik politikalarına ve standartlara uyum ve teknik uyum	2
24) Bilgi güvenliği yönetimi izleme ve denetimi	2
Toplam	**68**
Ortalama Değer	**2.83**

Seçilen Grup : Bilgi Güvenliği tedbirleri ORTA DÜZEYDE gerekli

	Kurumun aldığı Puan	Seçilen gruptaki ideal seviye puanı	Seçilen gruptaki ortalama seviye puanı
Toplam Puan	68.00 / 120.00 puan	101.28 / 120.00 puan	64.56 / 120.00 puan
Her bilgi güvenliği değerlendirme maddesindeki ortalama puan:	2.83	4.22	2.69

* Türkiye için ideal ve ortalama puanlar, ilgili grup için uzman görüşleri alınarak yaklaşık değerler olarak belirlenmiştir.



Kurumun Bilgi Güvenliği Yönetimi Genel Seviyesi : Ortalama Seviyede
Kurumunuzun bilgi güvenliği ihtiyacı : Orta Düzeyde
Bilgi güvenliği yönetim seviyesi grubunuzdaki ortalama düzeydedir.
Buna göre aşağıdakiler önerilmektedir:

- Bu seviyeyi korumak ve iyileştirmek için; kurum farkındalık ve bilinçlilik seviyesinin yüksek tutulması ve sürekliliğinin sağlanması. Bunun için yönetimi ve tüm çalışanları kapsayan kurum içi interaktif eğitim-çalıştaylar yapılması.
- Radar grafiği ve değerlendirme sonuçlarına göre; iyileştirilmesi gerekli hususların belirlenmesi, gözden geçirme ve iyileştirme çalışmaları yapılması. Bunu yaparken, uluslararası standartları (örneğin; ISO/IEC 27001 veya kurumun yasal olarak uyması gerekli benzeri standartları) dikkate almak yol gösterici olacaktır.
- Grubunuzdaki ideal seviyeye ulaşmanın hedeflenmesi.

Bilgi Güvenliği Yönetimi Değerlendirme Karnesi:

	Bilgi Güvenliği Yönetimi – Konu Başlıkları	Seviye
1	Bilgi Güvenliğine Kurumsal Yaklaşım	Ortalamadan Düşük Seviyede
2	Bilgi Varlıkları Güvenliği Yönetimi	Ortalamadan Düşük Seviyede
3	İnsan Kaynakları Güvenliği Yönetimi	Ortalama Seviyede
4	Fiziksel ve Çevresel Güvenlik Yönetimi	Ortalama Seviyede
5	Haberleşme ve Bilgi-İletişim Sistemleri İşletim Yönetimi	Ortalama Seviyede
6	Bilgi Sistemleri Erişim Kontrol, Geliştirme ve Bakım Yönetimi	Ortalama Seviyede
7	Bilgi Güvenliği İhlali Olay Yönetimi ve İş Sürekliliği Yönetimi	Ortalama Seviyede
8	Bilgi Güvenliği Uyumluluk ve İzleme Yönetimi	Ortalamadan Düşük Seviyede

	Bilgi Güvenliği Yönetimi - Hususları	Seviye
1	Bilgi güvenliği politikası	Ortalamadan Düşük Seviyede
2	Organizasyonel yapılanma	Ortalamadan Düşük Seviyede
3	Kurum içi ve dışı sözleşme-anlaşmalar	Ortalama Seviyede
4	Bilgi varlıklarının korunması	Ortalamadan Düşük Seviyede
5	Bilgi varlıkları sınıflandırması	Ortalama Seviyede
6	Bilgi varlıkları risk değerlendirme	Ortalama Seviyede
7	Bilgi güvenliği farkındalık ve eğitimi	Ortalamadan Düşük Seviyede
8	Bilgi güvenliği roller ve sorumluluklar	Ortalama Seviyede
9	İşe alınan ve ayrılan personel – güvenlik hususları	Ortalama Seviyede
10	Fiziksel güvenlik	Ortalama Seviyede
11	Kurum dışı kişiler- fiziksel güvenlik	Ortalama Seviyede
12	Ekipman ve techizat güvenliği	Ortalama Seviyede
13	Operasyonel bilgi sistemi güvenliği	Ortalamadan Düşük Seviyede
14	Zararlı yazılımlara karşı güvenlik	İdeal Seviyede
15	Bilgi iletişim ortamları güvenliği	Ortalamadan Düşük Seviyede
16	Bilgi sistemleri ve verileri erişim güvenliği	Ortalama Seviyede
17	Ağ erişimi güvenliği	Ortalama Seviyede
18	Bilgi sistemleri geliştirilmesi ve bakımı	Ortalama Seviyede
19	Bilgi Sistemleri güvenlik ihlali yönetimi	Ortalama Seviyede
20	Bilgi sistemleri olası arıza ve kesinti yönetimi	İdeal Seviyede
21	İş sürekliliği yönetimi	İdeal Seviyede
22	Güvenlikle ilişkili yasal yükümlülüklere uyum	Ortalama Seviyede
23	Güvenlik politikalarına ve standartlara uyum ve teknik uyum	Ortalama Seviyede
24	Bilgi güvenliği yönetimi izleme ve denetimi	Ortalama Seviyede

CURRICULUM VITAE

PERSONAL INFORMATION

Name, Surname : **Meltem Kocamustafaoğulları**

Nationality : **Turkish**

Birth date and place : **23.07.1966 – İstanbul, Türkiye**

Phone : **0312 4387127**

E-mail : **meltemk@kmo.com.tr**

EDUCATION

DEGREE	INSTITUTION	GRADUATION DATE
Computer Engineering (BSc)	Middle East Technical University	1987
High School	Fairborn High School, Ohio, USA	1982

WORK EXPERIENCE

YEAR	PROJECT	POSITION
1993 - present	KMO Information Systems	Founding Partner Technical Director
12/2012 - present	Ministry of Environment and Urbanisation - Technical Assistance (TA) for Implementation of REACH Regulation (EuropeAid /129602/D/SER/TR) KMO as Consortium partner	Local Project Director
12/2010-08/2012	Ministry of National Education (MoNE) - Technical Assistance for Strengthening the Statistical Capacity of MoNE (EuropeAid/126853/D/SER/TR) KMO as Consortium partner	Local Project Manager Quality Assurance Expert
01/2010-03/2011	KMO - Information Security Consulting Project (ISO 27001) Client name-confidential	Project Manager
03/2010-09/2010	Ministry of Interior, Border Management Unit – TA* for the Preparation of Border Surveillance Area Survey in Turkey (EuropeAid/127552/D/SER/TR) KMO as Consortium partner	Local Project Manager
07/2009-12/2010	Ministry of Environment and Forestry: Development and Maintenance of Environmental Information System – Extension (KMO)	Project Manager
11/2007-11/2008	Ministry of Environment and Forestry – Development and Maintenance of Environmental Information System (EuropeAid /123041/D/SER/TR) KMO as Consortium partner	Project Director
11/2006-11/2007	Turkish Customs Administration – TA* for analysis of Integrated Tariff Management System (ITMS) (EuropeAid/122780/D/SER/TR) KMO as Consortium partner	Key-Expert: Senior System Analysis and Design Expert

08/2006-11/2006	Judicial Modernisation & Penal Reform Programme Turkey (EuropeAid/123087/C/SUP/TR:)	Senior Evaluator
11/2004-07/2006	MASAK, (Ministry of Finance-Financial Crimes Investigation Board) TA on Strengthening the Fight against Money Laundering Project (EuropeAid/116585/D/SV/TR) KMO as Consortium partner (TA on establishment of Security Management System based on 17799, IV&V**and control-inspection of other Lots' project cycle & outputs)	Key-Expert: Senior Software Engineer Quality Assurance
05/2004-12/2004	European Union Centre of Training and Youth Program - Web Portal Design and Content Management System Project (KMO)	Project Manager & Team Leader
01/2004-12/2006	KMO Consulting projects for: TIB, DSI, PIGM, Emek Bilişim-Emekli Sandığı, SiemensBS, Yimpaş Holding	System Analyst Senior Technical Consultant
11/2002-05/2003	TETAS - Web Based Human Resources Management System Project (KMO)	Project Manager QA Manager
11/2000-12/2002	HUGO BOSS –AG Logistics System Project (KMO)	Development Team Leader
10/2001-06/2004	ORACLE Academy - Training Services (Oracle Certified Professional)	Instructor, Trainer
12/2002-05/2003	PIGM - Affairs; Migrating to Web Based Technology and Data Collection (KMO)	Team Leader
11/2001-12/2001	IGEME - Senior Consulting and Training Services for Foreign Trade Portal (KMO)	Senior Consultant, Trainer
05/2000-11/2010	POAS Petrol Ofisi (KMO)	Senior Consultant
08/1999-01/2000	PIGM - Design and Implementation of National Petroleum Information System Project (KMO)	Development Team Leader
08/2000-12/2000	TEPE HOME A.Ş. - Budget Management Datawarehouse System (KMO)	Project Manager
12/1995-12/1998	KMO ERP Projects for: HOSTA Textile, SARAR Group, EGS-Egeser, DYO Ortadoğu-KVK	Development Team Leader
01/1996-12/1998	KMO Consulting Projects for: Özaltın Group, CINE5, BEGENDIK	Senior IT Consultant
09/1993-12/1995	KMO –System Development Projects for: Bayındır Health Insurance, TOKI	Chief Developer
11/1992-09/1993	Deloitte and Touche World Bank funded, Turkish Standards Institute Financial MIS Project	IT Consultant
1991 – 1992	Consulting Projects for: Turkish EXIMBANK, EuroTech Gmbh, TUNA UCER	IT Consultant
08/1988-11/1991	Dogufaks (AT&T Value Added Reseller)	Technical Director
1987 – 1988	Cimhol Cement Comp.	IT Manager

*Technical Assistance, **Independent Validation and Verification

LANGUAGE

Turkish – Mother tongue, English – Excellent