THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

ASSESSING INFORMATION SECURITY MANAGEMENT REQUIREMENTS FOR FINANCE SECTOR USING AN ISO27001 BASED APPROACH

Master's Thessis

İZZET ATIL GÜRCAN

ISTANBUL, 2014

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
INFORMATION TECHNOLOGIES

ASSESSING INFORMATION SECURITY MANAGEMENT REQUIREMENTS FOR FINANCE SECTOR USING AN ISO27001 BASED APPROACH

Master's Thessis

İZZET ATIL GÜRCAN

Supervisor: Asst. Prof. Dr. ORHAN GÖKÇÖL

ISTANBUL, 2014

THE REPUBLIC OF TURKEY

BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
INFORMATION TECHNOLOGIES

Name of the thesis: Assessing Information Security Management Requirements for Finance Sector Using An ISO 27001 Based Approach
Name/Last Name of the Student: İzzet Atıl Gürcan
Date of the Defense of Thesis:

The thesis has been approved by the Graduate School of _____.

Graduate School Director
Signature

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

Program Coordinator
Signature

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

Examining Comittee Members	Signature
Thesis Supervisor Asst. Prof. Dr. Orhan Gökçöl	----------
Thesis Co-supervisor Assoc. Prof. Dr. F. Tunç Bozbura	----------
Member Asst. Prof. Dr. Yucel Batu Salman	----------
Member	----------

DEDICATION

To my all time supporters, my dear father; Zeki Gürcan, caring mother; Zeynep Gürcan and loving wife; Öznur Avutman. Special thanks to Çağatay Işıkçı for all contributions. Thanks to Orhan Gökçöl for guidance during this research.

ABSTRACT

ASSESSING INFORMATION SECURITY MANAGEMENT REQUIREMENTS FOR FINANCE SECTOR USING AN ISO27001 BASED APPROACH

İzzet Atıl Gürcan

Information Technologies

Thesis Supervisor: Yrd.Doç.Dr. Orhan Gökçöl

June 2014, 49 Pages

Information security management is a vital function in finance sector. Companies can face with different penalties if there are not any proper controls in place, in this highly regulated sector. These penalties may vary from simple financial payments to termination of business.

This research consists of a survey application which lets companies to compare their current information security management situation with an industry standard: ISO 27001:2013 and its results.

As a result, participants will recognize their maturity level when compared to highest possible options, and they also may position themselves in the finance sector overall. Another output of this study is to have participants find their strengths and weaknesses on ISO 27001:2013 certification and direct their investments based on these results.

Keywords: ISO 27001:2013, Information Security Management, Assessment

ÖZET

ASSESSING INFORMATION SECURITY MANAGEMENT REQUIREMENTS FOR FINANCE SECTOR USING AN ISO27001 BASED APPROACH

İzzet Atıl Gürcan

Information Technologies

Tez Danışmanı: Yrd.Doç. Dr. Orhan GÖKÇÖL

Haziran 2014, 49 Sayfa

Bilgi güvenliğinin sağlanması özellikle finans kurumları için hayati öneme sahiptir. Regülasyonlarla düzenlenen bu sektörde, gerekli önlemleri almamış firmalar çeşitli ceza müeyyideleriyle karşılaşmaktadırlar. Bu cezalar basitçe para cezaları olabileceği gibi kurumun iş yapış ruhsatlarının iptaline kadar gidebilmektedir.

Bu çalışma, kurumların mevcut bilgi güvenliği yapılarını endüstri standartlarından ISO 27001:2013 standardına göre karşılaştırmalarını sağlayan bir anket uygulaması ve bu uygulamanın sonuçlarından oluşmaktadır.

Çalışma sonunda, katılımcı kurumlar hem kendilerine ait olgunluk seviyelerini görebilecek, hem de finans sektörünün ortalamalarına göre nerede olduklarını tarafsız bir bakışla değerlendirebileceklerdir. Aynı zamanda çalışma sonuçlarına göre kurumlar olası bir ISO 27001:2013 sertifikasyonu için güçlü ve zayıf yanlarını görebilecek ve buna göre ilgili yatırımları gerçekleştirebileceklerdir.

Anahtar Kelimeler: ISO 27001:2013, Bilgi Güvenliği Yönetim Sistemi, Gereksinimler

TABLE OF CONTENTS

TABLES

FIGURES

ABBREVIATIONS

BIA:	Business Impact Analysis
BS:	British Standard
CIO:	Chief Information Officer
CISO:	Chief Information Security Officer
D-I-K-W:	Data, Information, Knowledge, Wisdom
FIPS:	Federal Information Processing Standards
GASSP:	Generally Accepted System Security Principles
IEC:	International Electrotechnical Commission
IT:	Information Technology
ITIL:	Information Technology Infrastructure Library
IS:	Information Security
ISM:	Information Security Management
ISMS:	Information Security Management System
ISO:	International Organization for Standards
NIST:	National Institute of Standards and Technology
NSTISSC:	National Security Telecommunications and Information Systems Security Committee
PDCA:	Plan – Do – Check – Act Cycle
RTP:	Risk Treatment Plan
SOA:	Statement of Applicability
SSL:	Secure Sockets Layer

1. INTRODUCTION

Understanding how to apply information security in accordance with best practices and evaluating current status of implementation for improvement can be critical for companies especially in governed sectors. To compare what can be done and what businesses did; first of all the definitions of information, security and information security should be done. After defining those terms; a management system should be selected for application. A survey should be conducted among specified sector. An analysis of survey results should be done for investigating the current situation and best practices. Difference between current situation and what should be done gives the ways to improve the necessary areas. A company then can use its people, procedures and processes for improvement and necessary certification.

In financial services sector, COBIT is a very common tool for assessing security. However the implementation can be very tedious because of the structure of COBIT. A rapid tool which gives an indicator of the IS infrastructure is highly demanded. As ISO 27001 is much easier for adoption, companies are questioned against selected clauses from controls from standard.

Even there are many companies in this regulated sector with government baselines applied; there are different sets of controls in each company. Motivation is to find the industry averages in a specific way so that companies in finance sector can assess their maturity levels with industry average and direct their future security investment to their weaknesses.

During the research basic terms are defined and management systems compared. After selection of a management system; a GAP analysis method is chosen for viewing the current situation. During the analysis; a maturity level scorecard is used for determining the company score over overall score. After defining the survey for analysis; this survey is applied to a set of financial institutions like banks, insurance, brokerage and pension companies. As it is a highly sensitive corporate data all the PII and commercial information is anonymized and gave the overall status of finance sector.

ISO 27001 way selected as the base standard as it has the easiest implementation between other standards and the most comprehensive management system. As the standard contains this method, GAP analysis is chosen for reviewing current situation. For every control objetive in ISO 27001 a 1-5 scale is used for determining the maturity level of implementation for this objective. So as more companies involve; companies can better position themselves in industry level.

Use of ISO 27001 in finance sector is not common and there are practically no extensive studies publicly available. In this study the aim is to use the easiness of the ISO 27001 standard to assess the readiness of the financial instutitions for a well-managed information security management system.

Weakness of this study occurs if the assessment is made by someone in the subject company. As the tool relies on objectiveness it is always a question mark if the user is objective enough or not. To avoid this conflict; either someone outside the company should do the research; or companies must understand the importance of objectiveness and act in a proper way.

2. LITERATURE REVIEW

Definitions are important for understanding which keyword is used for what meaning. There are three major terms which will be used in this research. So we must define each term by different sets of questions. Information. What is information refer to? How is it different from data? And how can we store it? Security. How is security defined? What are different types of security? And finally; information security. What are aspects of information security?

2.1 INFORMATION, SECURITY AND INFORMATION SECURITY

Data that is presented in a manner that is organized for a purpose in a timely manner is called information. [1] Also it has a value as it has affects on decisions or outcomes.

As per D-I-K-W approach; information is the structured data. Data is raw and it becomes information as people examine it. As people examine data, there happens to be a framework to understand the data represents. Information can be implicit, held inside our heads, or explicit, presented to public for utilization. Information only creates value when interaction with information produced by others occur. Information that is held by an individual, which is never revealed has no value. [2]

Generally, definition of security is "the quality or state of being secure to be free from danger". Which means, protection from who would make intentional or unintentional harm is the objective. There may be different levels of security for a subject. Corporate Security for example is a multilayered system. A system that protects the authority of a company, its assets, its resources and its employees. Getting the suitable level of security for a company also requires a sophisticated system.

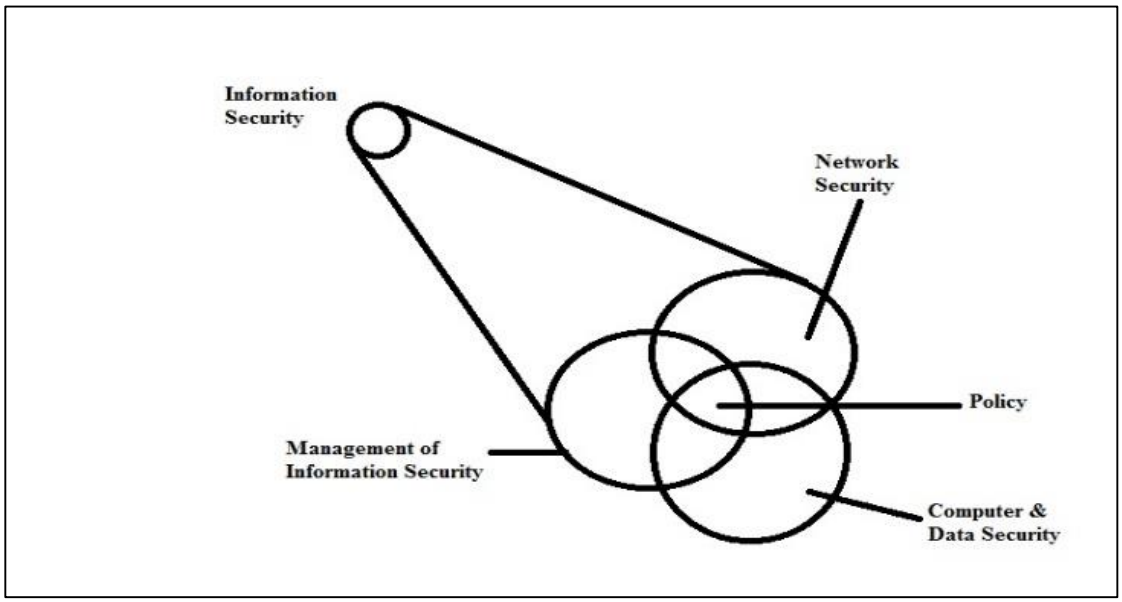
[1] Business Dictionary, 2013, [Online], http://www.businessdictionary.com/definition/information.html [date of visit: 20.June.2013]
[2] Spreading Science, DIKW Model of Innovation 2007, [Online], http://www.spreadingscience.com/our-approach/diffusion-of-innovations-in-a-community/1-the-dikw-model-of-innovation/ [date of visit: 20.June.2013]

As Michael Whitman and Herbert Matthord stated in their publication “Principles of Information Security”; successful organizations should have different layers of security in place to protect its operations:

a. There should be physical security measures in place for protecting physical items, objects zones from not entitled – unauthorized access.
b. Also there must be security measures for personnel security which aims to protect the individuals who are entitled to access the organization as well as its operations.
c. For protecting the details of series of activities from unauthorized individual or groups, there must be operational security measures.
d. For protecting all kinds of media, content and communication technology, there should be measures for communications security.
e. For protecting physical and logical connections, contents and other networking components, there should be network security measures.
f. For protecting the information assets in different perspectives such as C-I-A; even information asset is in storage (physical) stage as well as it is in operational (processing) or transmission (network) state; there should be information security measures. (Whitman & Matthord, 2011)

Protecting information from different threats to maximize business continuity and return on investments as well as minimizing risks related to business operations is called information security. It includes computer, data and also network security as there are different areas of information security management as shown in figure 2.1. (Aydoğmuş, 2010)

Figure 2-1: Components of information security



Source: Components of Information Security (Aydoğmuş, 2010)

Understanding IS management starts with understanding characteristics of information that makes it valuable. Value of an information is based on the C.I.A. triangle. Attributes of information that has importance are the basis of the CNSS model of information security. These attributes are confidentiality, integrity and availability which has been the standard for computer security for ages. However, up to date organizational needs made these three attributes alone insufficient because of scope limitations and can not cover the environment of the IT industry changed from day to day. With the change in industry, there are extended attributes and processes that includes identification, privacy, authentication, authorization and accountability. (Whitman & Matthord, 2011)

Confidentiality: Confidentiality means allowing access to the information from only those with a given need and proper privileges can access the information in question. Confidentiality protection measures include information classification, implementations of general security policies, secure document storage, education of end users and cryptographic controls. Confidentiality of information is extremely important regardless the type of organization and may be breached by either insiders or outsiders to the organization.

Integrity: Integrity is the state of being unaltered. Alteration, corruption, destruction or possible damaging threatens the integrity of data from its authentic state. This can happen

accidentally or as a result of more intentional behavior. Just like confidentiality; integrity of information can be threatened by both internal and external parties.

As stated in “User Efforts in Information Security” publication, there are different error control techniques to cover the internal and external threats. A common method for controlling integrity is called redundancy bits. After transmission of frames from network; error-correcting codes and hash values makes systems to ensure the integrity of the information. Data which is not verified during transmission is retransmitted or otherwise recovered (Beautament & Sasse, 2009)

Availability; third component of the C.I.A trianlge means the ability to access the information by authorized users without any interference when needed. The distributed denial of service attacks that occured in early 2001 show the importance of ability to access the information. (Greene, 2012)

Privacy: The privacy attribute does not involve freedom from observation but information usage ways known to person poroviding it. Which means an information collected from users is used by an organization only for the purposes stated to the data owner and at the time it was collected..

Many organizations treat personal information as commodity by collecting, swapping and spelling. It is now possible to collect and combine information on individuals form different sources, whose data might be used in ways not agreed to, or even not communicated to the data owner. Many people have become aware of these practices and are looking to government for protection for their privacy. (Whitman & Matthord, 2011)

Identification: Identity is a data set that has information on subject’s relationship to other entities and which has description of a person or an object uniquely. It is the first step in gaining access to secured material. Identification is typically performed by means of a user name or other ID that is unique to each and every individual, and serves as the foundation that is essential to establish the level of access or authorization.

Authentication: Authentication is the process of identitiy verification for a user, computer, grup, device, service or other identity. A good real life example of authentication happens when travelling internationally. As the passenger arrives to the airport, they present their passports to customs officers. Because customs trust the entity

that issues the passport; pasengers verify their identity in a reliable way. In digital life examples of authentication includes the hardware solutions like hardware tokens or biometric scanners but also software solutions like cryptographic certificates to establish Secure Sockets Layer (SSL) connections to confirm a user's identity.

Authorization: Authorization occurs after the authentication completes. It is the process that determines whether to grant or deny a user requested level of access to a resource (like access, update, or delete the contents). Access control lists and authorization groups in a networking environment and database authorization scheme to verify that the user of an application is authorized for specific functions such as read, write, create, and delete are examples of authorization.

Accountability: Accountability can be mentioned as the answerability of a named person or automated process. A common example of a system that provides accountability is audit logs that track the activity of a user.

2.2 INFORMATION SECURITY MANAGEMENT

Based on those definitions, information is an asset which has different values for different organizations. Information security protects information as well as the the facilities and systems that store, use and transmit it from a wide range of threats, for protecting its value to an organisation. This information security definition is tailored from the American National Security Telecommunications and Information Systems Security Committee (NSTISSC).[3]

Information Security Management System is an approach for managing information security with all involved business, people and infrastructure components included; at a high level in an effective way. Also ths approach cares about the continuity of business, poeople and infrastructure components involved. The aim of information security management system is reducing risks threatening informational assets to a manageable

[3] Open University, An Introduction to Information Security, 2013, [Online], http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-0, [date of visit: 15.August.2013]

level, while taking both business goals and customer expectations into perspective. ISMS is not limited to a specific industry. The concepts from information security management system can be applied with little changes to make it relevant to a specific industry. Information security management system is not a specific virus update, or a patch or a firewall rule set. It is the common sense behind what needs to go where. (Ramakrishnan, 2013)

Altough there are both internal and external threats to information assets of an organization; there are different standards and guides for managing the information security. Generally Accepted System Security Principles (GASSP) is an international workforce. Ten countries joined the workforce for raising a code, practice and procedure set for achieving information confidentiality, integrity and availability.

Also there is another organization for government agencies. Federal Information Processing Standards (FIPS) Publications provide baselines and regulations. Those rules are optional to privately held companies. Just like Federal Information Processing Standards, there is another international body available for private companies. International Organization for Standardization (ISO).

ISO has different certification standards for different needs of companies like ISO 9001:2008 Quality Management, ISO 22716 Good Manufacturing Practices. One of their standard covers the Information Security Management standard and adoptation guidelines for businesses. That standard is ISO 17799. Also there are different standards and checklists of best practices available as guidelines.

2.2.1 BS7799

In 1990's, a task force dedicated to information security was formed. The group published the "Code of Practice for Information Security Management" in 1993. That code of practice is registered as the BS 7799 in 1995 with some improvements.

After registration os BS 7799, the BSI formed a program called c:cure. C:cure was intended for authorization of conformity assessment and certification bodies as competent to audit to BS 7799. For the next update of BS 7799 in 1998, a steering

committee was set up. That committee updated BS 7799 in 1999, too. After the updates mentioned; standard now consists of two parts. Part 1 is known as “Code of Practice”, and Part 2 is known as “Specification of Information Security Management Systems”.

As stated in “Information Security Management: Understanding ISO 17799” book; understanding the differences between two parts of BS 7799 is critical. First part of the standard is based on suggestions. It is mostly an implementation guide and used for measuring and setting up the IS infrastructure. Second part is used as a guide for auditing based on information security management pre-requistes. For having BS7799 compliant certification, organizations are controlled against second part. Those controls are made by external comformity assessment and certification bodies mentioned before. Second part has details on what shall an organization do, while first one details IS concepts an organization “should” do. (Carlson, 2001)

2.2.2 ISO/IEC 17799:2005 Code of Practice For Information Security Management

ISO / IEC 17799 is a standard that used BS 7799 as a starting point. That is one of the most widely referenced security models. British Standard BS17799:2002 was reviewed in 2005. Output of that review is named as ISO/IEC 17799:2005 Information Technology Code of Practice for Information Security Management.

The purpose of ISO/IEC 17799:2005 is to issue manuals and setting foundational rules for triggering, maintaining, improving and implementing information security management. ISO/IEC 17799:2005 contains recommended applications for different subjects. Those subjects are called control objectives. Every control objective has different controls. Control objectives are listed below:

a) Security policy
b) Organization of information security
c) Asset management
d) Human resources security.

Human resources security includes the following subcategories.

i. Physical and environmantal security
ii. Communications and operations management
iii. Access control
iv. Information systems acquisition, development and maintenance
v. Information security incident management
vi. Business continuity management
vii. Compliance

Control objectives and controls are used to be deployed to cover the necessities of a previously made risk assessment. It is used as a fundamental component to improve organizational standards for information security as well as supplying practical guidance. ISO/IEC 17799:2005 also helps building confidence in inter-organizational activities. (Van Niekerk & Von Solms, 2010)

ISO/IEC 17799:2005 includes 133 possible controls. Some of topics include provision of outsourcing, external service delivery and patch management. Other areas including termination of employment and mobile communication have been modified and improved. Each section of ISO 17799:2005 includes four categories of information:

i. One or more objectives
ii. Controls relevant to the achievement of objectives
iii. Implementation guidelines
iv. Other information

ISO/IEC 17799:2005 is actually the final version of the original two-volume British Standard BS7799. Volume 1 offered an overview of the various areas of security and provided information on controls over 10 broad areas. Volume 2 provided information on implementing volume 1 and setting up an information security management system.

2.2.2.1 ISO/IEC 17799:2005 Clauses and controls

Some examples on ISO/IEC 17799:2005 clauses and controls are listed below. Full list of clauses can be found in appendices section.

A.5 Security policy

A.5.1 Information security policy

“Management should define a policy to clarify their direction of, and support for, information security, meaning a short, high-level information security policies tatement laying down the key information security directives and mandates for the entire organization. This is normally supported by a comprehensive suite of more detailed corporate information security policies, typically in the form of an information security policy manual. The policy manual in turn is supported by a set of information security standards, procedures and guidelines.”

As seen on standard, first clause of ISO/IEC 17799:2005 is about having security policy in place with a management support. It is the first step of implementation; to have an information security policy with management support. Without proper management support; no policy is enforced in the company environment. Full list of sections in ISO/IEC 17799:2005 can be found in Appendix A.

2.2.3 ISO 27001

ISO 27001 standard is a standard replacing the old British Standard 17799-2 by enhancing its content. ISO 27001 is the specification for an ISMS. A scheme for converting from BS7799 certification to ISO 27001 certification is introduced by various certification bodies.

Objective of ISO 27001 is providing a model to establishing an Information Security Management System. It also has objectives to support for implementation, operation, monitoring, maintaining, reviewing, and improving the management system. Adoptation of the standard is a strategic decision involving management and senior management. Furthermore; design of an organizations information security management system is lead by organizations needs, size, objectives and structure. The process employed and their security requirements has also affect in the design as well as the implementation of information security management system. (the ISO 27000 Directory, 2013)

Standard is based on a process approach and uses the Plan – Do – Check – Act (PDCA) model which is deprecated in 2013 revision of standard, for structuring.

2.2.4 ITIL

ITIL (Information Technologies Infrastructure Library) consists of five core volumes for IT Services Lifecycle. One of the five core volumes; Service Design includes a process for information security management. That process describes structured fitting of information security in the management organisation.

Code of practice for information security management system which is also known as ISO/IEC 27001 is the core of this process in ITIL.

The goal of Information Security Manageent Process is to line up IT Security with business needs and making sure that information security is managed efficiently in all activities related to the service and service management. Information security is a management activity which is in the corporate governance framework.

Corporate governance framework provides the strategic direction for security related activities and ensures that objectives of corporate governance are achieved. Appropriate risk handling of informational assets and responsibly using of enterprise information resources are also concerns of corporate governance framework.

It is meant to providing a focus for all aspects of IT security and manage all IT security activities. (OGC, 2013)

2.2.5 NIST Security Models

Other resources for information security management practices is available at NIST Computer Security Resource Center documentations. These documents have two major advantages over other practices:

a. They are available to public without any charge.

b. NIST models are available for some time, which means they are reviewed by many government and industry profesionals.

NIST Documents aims to help designing a custom security framework for the organizations information security program.

2.2.6 COBIT

COBIT 5 outline is used to develop information security structure. It emphasizes on securing assets and gives guidance based on experiences. Even it has different explanations available on literature, this particular one is important as it covers the three major attributes of an asset: CIA.

The term "integrity" is covered in the information enabler as information goals of intactness and precision. Rigorously related to stakeholder confidence; either by pointing out business risk or by generating value for an enterprise, information security turns out to be a business enabler for organizations.

2.3 ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

Need for information security is increased from time to time with the broadening of communication in different ways. It is not possible to secure information with just using of technical countermeasures like firewalls or anti virus software as seen before. Not just those technical countermeasures but there is an increasing need for a management system; which consists of people, processes, procedures and information systems that is supported by business management.

Information security standards are developed to protect business processes from risks on information security, to have countermeasures applied systematically and to certify the companies which are compliant to those assesments. (Vural & Sağıroğlu, 2007)

2.3.1 What is ISO 27001

Protection of information assets, mitigation of possible risks and continuity of business processes can be accomplished by implementing an ISMS with management support. ISMS is a management system anticipated by ISO 27001.

Due to standard, all management systems related to information security are made to get management in direction of information security. ISMS includes the company structure, planning activities, company policies and responsibilities, applications, processes, procedures and resources. ISO 27001 standard document is used for accomplishing enterprise information security. It is also developed to be applicable to organizations of every size. It does not just deals with technical system security but overall information security.

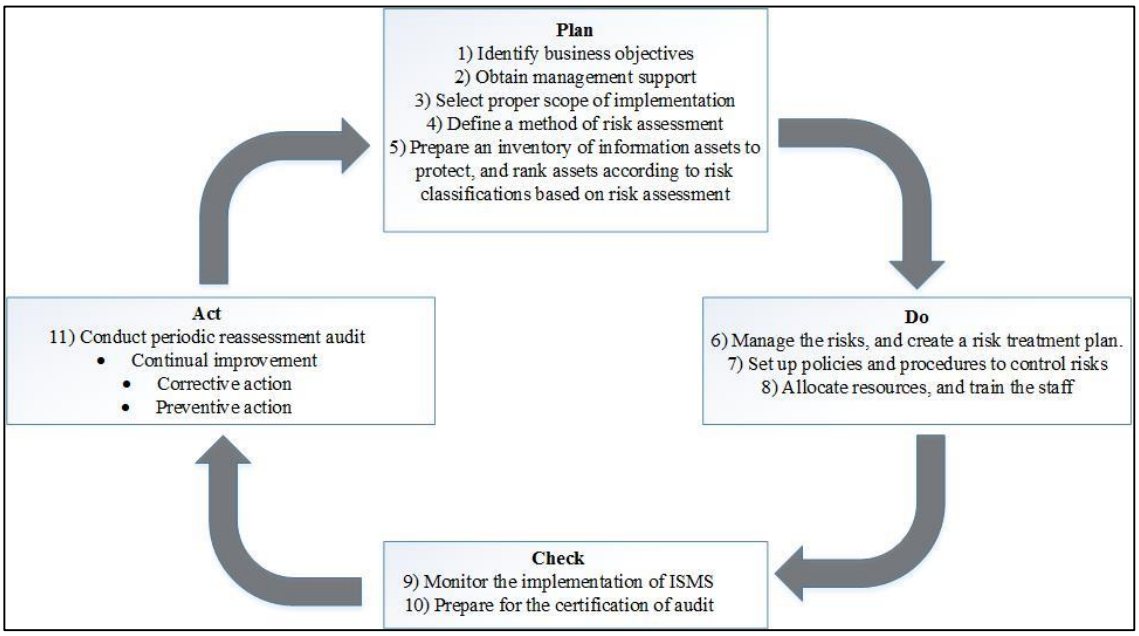
ISO 27001 standard is prepared for implementing, realizing, operating, reviewing, continuing, and enhancing the Information Security Management System as a model. It is a strategic decision for a company to internalize the ISMS. The ISMS concept and execution of a company is affected by the needs of the organization, security prerequistes, processes used, the structure, goals and the size of the business. Change in those factors and supportive systems is expected in time. Also an ISMS is expected to scale due to changing needs of a company.

ISO 27001 is a process based standard. Every activity for having an output from an input is considered as a process. ISO 27001 has the following processes:

a. Understanding need for business information security and understanding the need for information security policy.
b. Having controls for managing risks of information security in managing overall risks for company.
c. Inspecting the performance of management system and reviewing the performance as well as its utility, when necessary.
d. Regular enhancement of management system based on measurement of KPI's.

ISMS should be a living process. As a result; standard is based on PDCA cycle for Information Security Management System. PDCA cycle applied to ISMS processes can be summarized as shown in figure 2.2.

Figure 2-2: PDCA cycle



Source: PDCA Cycle (Pelnekar, 2011)

Plan: Planning phase is the execution phase of ISMS. Scope for management system, ISMS policies of company, targets, processes and procedures related to policies is created in plan phase. Milestones in "Plan" phase are listed below:

a. Defining the ISMS scope.
b. Defining the ISMS policy.
c. Defining risk assessment approach.
d. Risk identification.
e. Risk assessment.
f. Identification and evaluation of options for the risk treatment.
g. Selection of necessary control objectives and controls.
h. Preparing a Statement of Applicability (SOA).

Do: Do phase includes realizing the management system and operating the ISMS. Operating the ISMS means, operation of policies, controls and processes as well as procedures. Steps in "Do" phase is listed below:

a. Formulation of Risk Treatment Plan.
b. Executing the Risk Treatment Plan.
c. Executing necessary controls.
d. Executing training and customer awareness programs.
e. Managing the operations.

f. Managing the resources.
g. Implementing procedures for detecting and responding to security incidents.

Check: Monitoring the management system and inspecting it is the check phase. Also evaluating process performance based on policies, measuring where available and reporting to management for evaluation.

a. Executing the monitoring procedures.
b. Undertaking regular inspection of management system performance.
c. Inspecting the level of residual risk and acceptable risk.
d. Conducting information security management audits internally.
e. Undertaking regular management reviews for the management system.
f. Recording actions that has impact on management systems as well as events that trigger those actions.

Act: Continuity and improvement of ISMS is the Act stage. Ensuring the information security management system continuity by making corrective and preventive actions according to the review reports for management.

a. Implementing the identified improvements.
b. Taking corrective actions or necessary preventive action.
c. Applying the lessons learned.
d. Communicating results to interested parties.
e. Ensuring improvements to achieve objectives.

Plan, do, check, act stages follow each other as a cycle and creates a living information security management system.

According to the certification institution, the proposed use of ISO 27001 is;

i. Internal usage in organization to formulate objectives and business security requirements.
ii. Internal usage in organization to make sure a way to make sure that security risks are handled in an economic manner.
iii. Internal usage in organization for make sure organization is compliant with laws and regulations.
iv. Internal usage in organization as a structure for processes for the execution and management of security controls to make sure security objectives specified in scope of the organization are met.

v. Definition of new security management processes.
vi. Recognition and clarification of existing IS management processes.
vii. Management usage for organizations to understand the state of ISM activities.
viii. Internal and external auditor usage for determining the level of policy compliance, standards and directives of an organization.
ix. Internal usage of organization for providing information about IS that has relevance to security policies, procedures, standards to businesses that has partnership with and other concerning third parties.
x. Providing information about IS that has relevance to customers.

2.3.2 ISO 27001 Implementation

Companies should identify informational assets at first place to establish an enterprise information security management. Which means informational asset inventory should be made. This is how a company can list their assets, understand the risks that affect those assets, and foresee how business is impacted if a particular asset is missing. That will make the value of asset. As a next step; companies should identify how to protect which asset against which risk. This results in identification of informational assets and information protection costs.

Assets that are valuable to company should only be protected as their value continues and the cost for protecting those assets should not be higher than the value of asset itself. Main purpose of this principle is not to protect meaningless assets. Also another purpose is not to spend more than recovery / renewal cost for protection, if the asset is damaged or lost. Implementation of ISMS consists of asset management, risk analysis against this assets, building security policies, audit and applications of controls and maintaining system by developing necessary solutions.

2.3.3 Steps of ISMS Implementation

Implementing an Information Security Management System consists of important steps like team forming, scope identification, and asset value determination just like given in

table 2.1. Those steps also includes risk assessment process which is very important for both ISMS and the business.

Table 2.1: Mapping ISO 27001 suggested steps to implement phases

Mapping ISO/IEC 27001 Suggested Steps to Implementation Phases	
ISO/IEC 27001:2005 Suggested Steps	Implementation Phases
Define an ISMS Policy	Phase 1: Identify business objectives Phase 2: Obtain management support
Define the scope of the ISMS	Phase 3: Select the proper scope of implementation
Perform a security risk assessment	Phase 4: Define a method of risk assessment
Manage the identified risk	Phase 5: Prepare an inventory of information assets to protect, and rank assets according to risk classification, based on risk assessment.
Select Controls to be implemented and applied	Phase 6: Manage the risks, and create a risk treatment plan Phase 7: Set up policies and procedures to control risks Phase 8: Allocate resources, and train the staff
Prepare an SOA	

Source: Mapping of ISO 27001 suggested steps to implement phases, (Pelnekar, 2011)

2.3.3.1 Team formation

Steps to establish an information security management system starts with forming a team. A primary connection between the implementation team and senior management called Chief Information Security Officer (CISO). Role is responsible for getting approvals and making decisions on behalf of management in a formal way. (Zakaria, 2009)

Also a user will be in charge of the project and will be reporting to Chief Information Security Officer should be in team. That role is called as project manager or as Information Security Officer (ISO). Also there should be other team members from every department within the ISMS scope.

2.3.3.2 Defining the Scope

ISMS can be implemented for a department, a branch or the entire organization. Implementation team should agree on the areas of information security management system with senior management. Those areas are defined as the scope of Information

Security Management System. This should be clearly defined in Information Security Policy Document.

As soon as the scope is defined, business processes of departments in scope should be understood for better alignment of ISMS with business. To accomplish this alignment, one member from all departments in the scope is added to the implementation team.

For each and every business process studied in the scope, a document called Business Process Study can be prepared. This documentation is not mandatory in ISO 27001 standard but will help in later stages for identifying assets and identifying values for these assets.

2.3.3.3 Risk assessment and risk management

ISO does not force the method to be used for analyzing the risk, even it forces the risk analysis to be made. Organizations can not be certified as compliant without proper risk analysis and proper counter activities. Businesses may characterize and write down a method of their choice. Usable risk analysis should have the following details in place;

a. How to analyze the risk of companies assets.
b. Understanding the risks that have small effect on business operations thus disregarded and understanding the risks that have high effect on business operations thus need to paid attention to.
c. Handling remainder risks by executing proper controls.

Risk evaluations are based on three attributes of an asset. Those are the ones known as CIA. Confidentiality, Integrity and Availability of assets is detailed within the standard as below:

Confidentiality: With confidentiality attribute of an information asset defined in clause 3.3; organizations make information reachable to users who need to reach with a proper business cause.

Integrity: Integrity attribute of an information asset defined in clause 3.8 controls the protection of validity and totality of information and information processing method.

Availability: Availability attribute of an information asset defined in clause 3.9 makes sure that the access to information asset is done by only authorized users who have explicit access to resources when necessary.

2.3.3.3.1 Preparing of an information asset inventory, asset ranking and risk classification

After formation of implementation team and definition of the scope, information assets on scope should be identified for proper risk assessment. Also if there are some legal or regulatory requirements; or requirements based on contracts are present, those requirement should be identified properly.

Identified assets can either be information assets or data asset, people or service asset, technology asset or service asset (i.e. people, procedures, data, software, hardware and network assets). For listing those assets in a risk management perspective:

a. People are divided into insiders (employees) and outsiders (non-employees). Insiders come in two categories: either they hold trusted roles and have correspondingly greater authority and accountability; or they are regular staff without any special privileges. The group of outsiders consists of other users who have rights to reach out to the organization's assets.
b. Procedures are assets. They are split into two categories: IT and business standard procedures, and IT and business sensitive procedures. Sensitive procedures have the potential to enable an attack or to otherwise introduce risk to the organization. Both groups of procedures are used to create value to organization.
c. Data components are named for information in all states: in transmission, processing, and on storage. These categories expand the conventional use of the term "data", which is usually associated with databases not the full range of information used by modern organizations.
d. Software elements can be inventoried in one of three categories: applications, operating systems, or security components. Software components which provide security controls like anti-virus or software firewall systems may fall into the operating systems or applications category, but those are differentiated by the fact that they are part of the information security control environment. And as they provide security; they must be protected more thoroughly than other software components.
e. Hardware can split into two categories; systems devices and their peripherals, and the devices that are part of information security control systems. The latter must be protected more thoroughly than the former.

f. Networking components are differentiated from both software and hardware because they are often the focal point of attacks against a system. (Aydoğmuş, 2010)

Labeling the assets and values are best practices for creating an information asset inventory.

Asset values are identified by their confidentiality, integrity and availability impact levels of an asset such as high, medium and low. After identifying the values of an asset; identification of risk and classification based on their severity and vulnerability is done . As the identification of the risks and CIA levels of an asset completed, values for risks should be assigned. Based on the risk values; tolerance of risk or need to implement a control for reducing or eliminating a risk should be determined.

As the risk assesssment is finished, business can identify what to do for protecting the information assets that have high effect on business operations and thus need to paid attention to.

2.3.3.3.2 Business impact analysis

Based on the identification of information assets of needs and requirements a risk assesment must be made. Risk assessment is a two phased process. First of all a risk value should be calculated. The risk value of an asset is determined by identifying possible threats to CIA attributes of asset, how much will business be effected without the asset and how often may the harm be. This parameters also leads us to Business Impact Analysis.

BIA is done for analyzing the effect of a loss of and asset because of different possible reasons. Risk assessment and risk analyze will help businesses understand the possible weaknesses and hazards to system and how will be business effected with those harms, where BIA is based on time. Time that a business can go and how the business continues its operations without that asset if there is a failure on an asset is derived by the business impact analysis. (Zakaria, 2009)

As each information asset is assigned to its proper priority, asking some simple questions can help to improve the criterion. This criterion will be used for valuation of assets. Also this criterion will be used for understanding the effects of a possible business impact.

i. What information asset is the most critical asset for business operations?

ii. Greatest revenue is generated by which asset?
iii. Highest profit is generated by whşch asset?
iv. Replacement of which asset costs the highest?
v. Protection of which asset costs the highest?
vi. Loss of which asset would create the biggest issue?

After identifying the values of assets and the business impact, probability of occurance is needed for identifying the risk value. Probability of occurance is shaped by expertise as well as the present situation.

2.3.3.3.3 Managing the risk

After calculation of risk values with asset values, management should decide which assets are subject to reduction of risk. This must be done as some controls to reduce the risks may cost more than the asset itself. For controlling the effect of possible harm to business, organization should either accept, avoid, transfer or reduce the risk to a lower level using controls that reduces the risk.

Next stage is to analyze the current state with the controls provided in the standard for creating a RTP and a SOA document.

Information on how to handle the risk to a lower level as well as understanding of operational controls and any additional controls are listed in RTP as well as possible execution time frames. Example shown in table 2.2. There are different methods for handling risks like:

i. Risk acceptance: Understanding and accepting risk, continuing operations or implementing controls for lowering risk where risk level can be accepted.
ii. Risk Avoidance: Evading risk by removing the reasons.
iii. Risk Limitation: Risk limitation is used to lower the adverse impact by executing necessary controls to an asset.
iv. Risk Transfer: Risk transfer is used to compensate for the loss in the event of risk is happened. (i.e. insurance)

Table 2.2: Risk treatment plan with applicable controls

Risk	Explanation of Risk Treatment Categories			
	Reduce	**Avoid**	**Accept**	**Transfer**
Information Security Risk	Try to decrease the risk; use the controls for understanding and executing a proper IS Control.	Keeping away from the risk by proper planning scheme, recreating the designing scheme.	Management must understand the exess risk in case of unavailability of a resolution.	Search for options for transferring the whole or a part of the risk to a third party (insurer)?

Source: Risk treatment with controls (Pelnekar, 2011)

After deciding the risk management strategy, a Statement of Applicability (SOA) should be written for ISMS implementation. SOA is a document which lists the ISO 27001 controls and their implementations with proper justifications. A justification should also be listed if a control is not selected. The document is to be presented t internal and external parties on demand. An example for headers of an SOA document is shown at table 2.3.

Table 2.3: Example SOA headers

Control Reference	Description	Implementation	Justification
A.9.2.2	Fire Supplies	Yes	Have UPS systems and a dedicated generator
A.10.4.1	Malicious Code	Yes	Implemented centralized anti virus server

Source: Example SOA headers (Pelnekar, 2011)

As the SoA document is written and all the policies, standards and procedures to implement the controls are defined requirements for ISMS documentation can be completed

2.3.3.4 Setting up policies and procedures

For controls that are adopted or implemented as listed on statement of applicability document, organizations will have to define policies and course of actions and possible roles and responsibilities for stable execution of planned policies and procedures. Writing down the policies is a requirement of ISO 27001. (Pelnekar, 2011)

2.3.3.5 Allocate resources and train the staff

ISMS Emphasizes one of the management missions that has significant importance. Dedicating the necessary facilities and people for development, execution, and management of the isms. It is fundamental to write down the training for the ISMS audit.

2.3.3.6 Monitoring the implementation

In-house audits are must-do's for inspecting and reviewing the ISMS execution. In-house audit includes testing and having improver / protective actions for those tests. For completing the PDCA cycle, gaps found during audits should be covered by understanding and executing improving and protecting controls that are based on analysis. And update the necessary documentation.

2.3.4 ISO 27001:2013 Revision

With the 2013 edition, there are some slight differences made to the standard itself. Some controls have changed and some merged together. Terms and definitions part is deprecated in 2013 edition. ISO 27001 edition of Terms and Definitions refer to ISO/IEC 27000 standard. Most important change in standard is there is no need for PDCA model any more as continual improvement occurs. Also there is a shift to move support of the ISMS to the executive management level.

Risk management section is aligned with the ISO 31000 standard. There is a new concept of Risk Owner and the management of risks has higher focus then the control effectiveness. Also there is no need for identifying assets, threats and vulnerabilities before risk identification. With the alignment of ISO 31000; risk management section now discusses consequences instead of impact. Preventive action in risk management no longer exists but is replaced by "Risks and Opportunuties". Also determination of controls is now a part of risk assesment instead of Annex A. But the need for validating selected controls from Annex A exists.

Goals for changes in ISO 27001:2013 edition is listed below:

i. To align the structure of all ISO 2700x family and the management standards including shared language for all non-specific components in management systems.
ii. Clarifying the requirements and content of isms..
iii. Revising and improving the information securty management system technical requirements.
iv. Revising and sustaining the additional controls. And conformance with Annex SL requirements.
v. Correcting errors, removing the recurring controls in different sections.

When the scope of 2013 edition is compared with 2005 (standard clauses 1-8 and Annex A), document is shortened to 22 pages fom 29 with a decrease of %25. This decrease is accomplished by removal of the recurring and unnecessary standard clauses, Annex B and Annex C.

Requirements of an ISMS is revised in technical and structured manner. Standard clauses in 4-8 sections of 2005 edition is revised and improved as a new framework. New clauses listed in sections 4 – 10 is listed below.

Context of the Organization (Clause 4)

Leadership (Clause 5)

Planning (Clause 6): includes planning the information security management system, setting the acceptable risk level and setting the risk evaluation methodology.

Support (Clause 7): includes preparing supportive and collateral resources for ISMS implementation, preparing for end user abilities and awareness, trainings, fulfillment of documentation needs and communicating with involved parties.

Operation (Clause 8): includes operation and management of ISMS implementations, sustaining evaluation, improvement and risk assessments.

Performance Evaluation (Clause 9): includes evaluating controls and information security management system with audits, metrics and management review.

Improvement (Clause 10): includes continuous improvement on ISMS.

Tight relations with PDCA model in 2005 edition is no longer exists. This does not mean that a PDCA cycle does not exist or can not be used[4]. (Kosutic, 2014) Sections in 2013 edition can be matched with PDCA cycle steps as listed in table 2.4.

Table 2.4: Matching of PDCA steps with sections in ISO/IEC 27001:2013

<table>
<tr><th>PDCA</th><th colspan="2">Sections in 27001:2013</th></tr>
<tr><td>Plan</td><td>4. Context of Organization
6. Planning</td><td rowspan="4">5. Leadership</td></tr>
<tr><td>Do</td><td>7. Support
8. Operation</td></tr>
<tr><td>Check</td><td>9. Performance Evaluation</td></tr>
<tr><td>Act</td><td>10. Improvement</td></tr>
</table>

Source: Dejan Kosutic, Has the PDCA Cycle been removed from the new ISO standards?, April, 2014

Total of 133 controls were listed in Annex – A of 2005 edition decreased to 114 controls in 2013 edition. Some controls like A.12.5.4 Information Leakage and A.11.5.6 Limitation of connection time are removed completely and some of the controls like Malicious and mobile code is combined to A.12.2.1 Malware. Also there are new controls added to the standard. Those new controls and sections in 2013 revision are listed in Appendix B.

Every risk has an owner in 2013 edition. Asset owner concept in 2005 edition is revised as the risk owner. Risk owner will be responsible for risk mitigation plan and acceptance of risks. Risk management documentation is not necessary in 2013 edition but the process of risk management should be defined.

2005 edition had 5 mandatory procedures but 2013 edition has removed the explicit requirement. Although there is still a requirement for documenting controls including supporting records. Internal audit is still required but it no longer requires a formal procedure.

[4] ISO27001 Blog 2014, [Online], http://blog.iso27001standard.com/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/ [date of visit: 14.April.2014]

Management review no longer defines specific precise inputs and outputs but provides a list of topics that needs to be considered and must occur at planned intervals. At least annually.

Annex B in 2005 edition contained cross references to the OECD principles. Also referred to the PDCA model which no longer exists. Because of these; there is no equivalent annexure in 2013 version. (Simpson, 2014)

Annex C provided a cross reference between 27001 and other standards. But as the other standards in this section is revised, this annexure is removed with no replacement.

2.4. A CASE STUDY FROM FINANCE SECTOR:

An accounting firm from Great Britain Brookson, figured that ISO 27001 certification would be a business differentiator and a great way to demonstrate a best practice approach for safeguarding client data and IT systems that the services rely upon. As they give accountancy services to their customers both from call center and online real time accounting and tax query services as a differentiator; accessibility attribute of data is highly important in their client satisfaction. Their services should keep being compliant and should maintain high level of client satisfaction.

Primary business driver for setting up an isms was an internal decision for adopting best practice in maintaining the CIE of information and information assets. Despite other examples which gets pressurized by a group of stakeholders or customers on adopting a management system, Brookson received no external pressure. They have identified the importance of adopting a continuous improvement model for protecting both client data and company reputation proactively.

Even Brookson owned the planning and deployment of isms, they wanted to have assistance from a certified consultancy company. Their chosen partner made a high level presentation to project team about the key stages and implications of certifying. During the deployment phase, brookson got the ownership but appreciated having consultant available and accessible for guidance.

Brookson determined the scope of isms to IT services as they are providing critical services to managed customers which is served by their It infrastructure. As the scope is set as IT services; company wanted to have all employees to have benefits of having iso 27001 certification.

Even Brookson adopted different risk based approaches across a variety of projects, there were no formal security related risk assessment has been conducted. Brookson found their consultancy companies risk assessment tool benefical. Before assessment Brookson thought that all the risk is internal but after assessment, they had a greater awareness of external factors like environmental and legal.

Another positive result of risk assessment was having senior management involved in process. Final result of risk assessment was the risk treatment plan which is signed by the managing director so prioritization of different treatment for different risks occured.

Even the certification is limited to information technologies; all the policies and processes were implemented consistently and comprehensively across all organisation. For communicating the policies and presentation of certification; Brookson used its typical fun ways. There were different methods used like mastermind quizzes with a cartoon character where it appeared for reinforcing good practice in areas such as clear desk and clear screen policies.

Information security was seen as having organization wide important event the scope was limited to IT. With the company launch and a series of internal presentations, staff become more aware of the importance of IS and the potential impact on Brookson.

Brookson always treated client data with considerable care and diligence. However partnering with a third party risk assessment company made the company validate the best practice used.

One of the processes improved by the implementation was incident management thus incident reporting. Before the implementation Is incidents were reported with other issues. As ISO 27001 developed a PDCA model; Brookson developed a new incident reporting process for corrective and preventive action process.[5]

[5] (Study, 2012)

3. DATA AND METHOD

3.1 SURVEY INFORMATION

For assesing the requirements for information security management system of companies in Turkey finance sector; an online survey is conducted. Survey aims to figure maturity level of attending company in information security management system. Survey is listed on following webpage:

Survey consists of 61 questions. Those questions belong to a different control categories in ISO/IEC 27001:2013. Each question is based on a likert scale from 1 – 5 with values between 0-4. Answer definitions and values are listed in table 3.1.

Table 3.1: Maturity levels and values of each answer

Level	Maturity level in one to five scale	Value
1	**No awareness** about the control or **no countermeasure rules** are established	0
2	Management is **aware of the control** and **will establish** a rule in the **future.**	1
3	Necessary **rules and controls are being established** with the approval of management. **But no review has been made.**	2
4	Necessary **rules and controls are established within the scope** aligned with management leadership. **No review of controls has been made.**	3
5	Necessary **rules and controls are established** within the scope with management leadership. **Review is made on a regular basis**.	4

For each ISO 27001:2013 section, points based on attendants answers are compared with the maximum available points for that section and maturity level for that section is calculated. All the PII data is anonymized and the contact information is held for sharing the results if the attendant is agreed to.

Even the survey is made in Turkish; an example of questions and referenced control categories is given in table 3.2. Full list of survey questions and their referenced ISO 27001:2013 clauses are listed in appendix c.

Table 3.2: Example list of survey questions and related ISO 27001:2013 sections

Statement	Cont. Cat.
There is a defined policy in place, approved by management and reviewed by authorities in planned intervals.	A.5.
Roles and responsibities in information security are defined and segregated properly, communicated with the authorities or other third parties	A.6
Information security is applied in project management?	A.6
There is a policy for mobile devices and managing the risks involved with mobile device usage.	A.6

For every section, attendants answers have a total value and this number is compared with the total value of each section. Total maximum score for each section is listed table 3.3.

Table 3.3: Maximum available scores per section

Section	**Section Name**	**Total Maximum Score**
A.5	Information security policies.	4
A.6	Organization of information security.	16
A.7	Human resource security	16
A.8	Asset management	20
A.9	Access control	24
A.10	Cryptography	8
A.11	Physical and environmental security	36
A.12	Operational security	32
A.13	Communications security	16
A.14	System acquisition, development and maintenance	20
A.15	Supplier relationships	8
A.16	Information security incident management	12
A.17	Information security continuity	12
A.18	Compliance	20

Results are given as rational numbers with attendant score / section total. This result reflects the attendants maturity level, as well as the total maturity level of finance sector in Turkey.

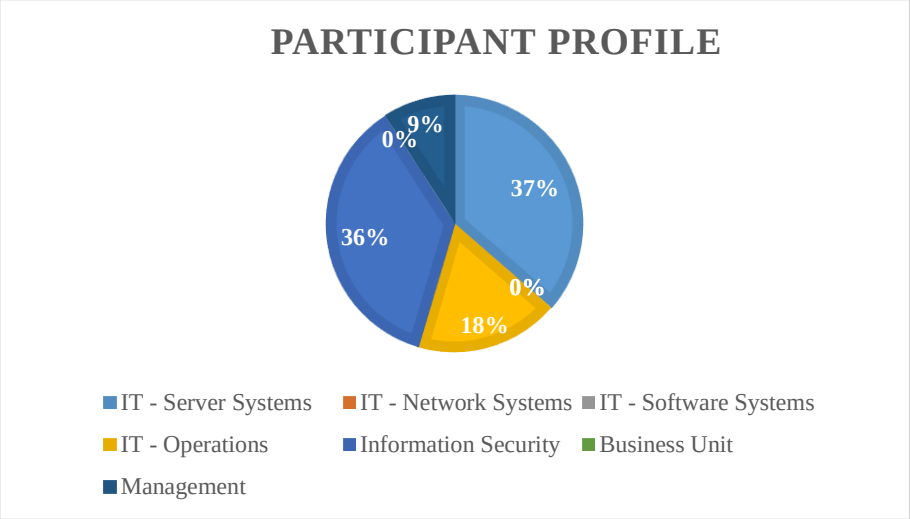
3.2 PARTICIPANT PROFILE

Survey is conducted among 11 different companies in financial services sector. Participants are chosen by the company itself and vary from C-Level management to IT Staff. Detailed information on participants and their visualization with a pie chart is given in Table 3.4 and Figure 3.1.

Table 3.4: Participant Role Details

Participant Role	Count
IT – Server Systems	4
IT – Network Systems	0
IT – Software Systems	0
IT – Operations	2
Information Security	4
Business Unit	0
Management	1

Figure 3-1: Participant Profile Visualization



According to the Banks, Branches and Employees Report of june 2014 from the Banks Association of Turkey[6]; there are 46 banks in Turkey with a total branch of 11.137 and a total of 198.894 employees.

If we exclude the investment banks and the banks who has branches under 10; remaining banks which are for banking deposits is 22. Those deposit banks have a total branch number of 11.089 and have 194.737 employees working.

When we look at the numbers of the banks who participated to ISO 27001 maturity level survey; those are 11 banks with 6503 branches and 108.365 employees. Detailed information can be found in table 3.5.

Table 3.5. Ratios of Banks Participated to Survey to Total Number of Banks

	Number of Banks	**Number of Branches**	**Number of Employees**
Sector Total	46	11.137	198.894
Number of investment banks and branches under 10	24	48	4157
Banks that accept deposit	22	11.089	194.737
Banks that participated to survey	11	6503	108365
Ratios	**50%**	**59%**	**56%**

As seen on table 3.5; eleven participants have almost 60% of branches in Turkey and covers more than half of financial workers in Turkey. Related table from banks, branches and employees report can be found in appendix d.

[6] (Association, 2014)

4. FINDINGS

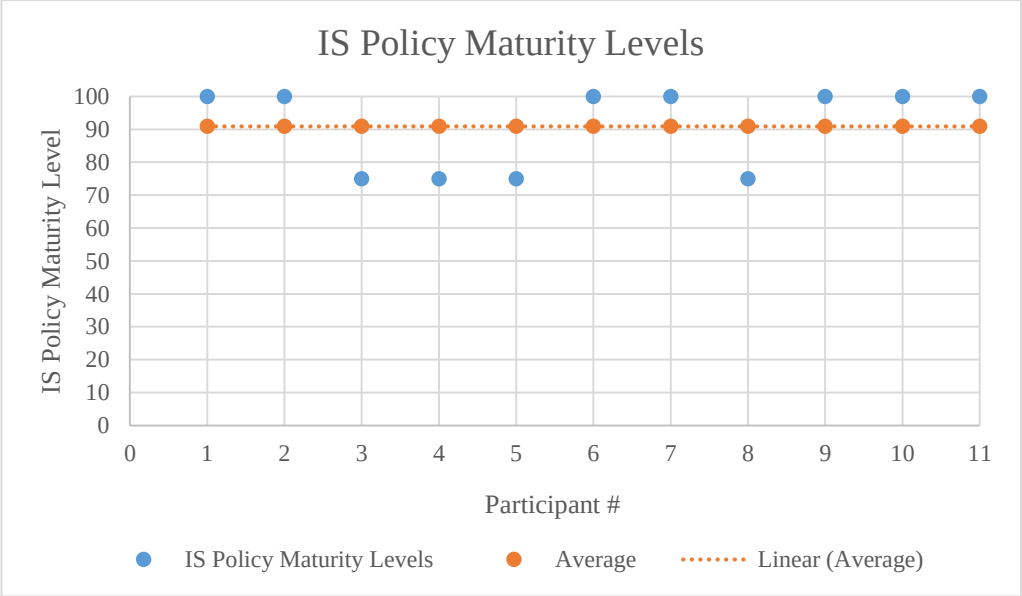
Survey questions with scores derived from answers of participants related with different control categories is reviewed in this section.

4.1 IS POLICY MATURITY LEVELS (A.5)

Looking at the answers given by the participants; we can see that there is an information security policy document exists in every attendant. Most of the attendants are reviewing this information security policy document at planned intervals (7) but some of them (4) not.

Visualization of maturity levels for participants based on their answers for IS policy related survey items is listed in figure 4-1.

Figure 4-1: IS Policy Maturity Levels

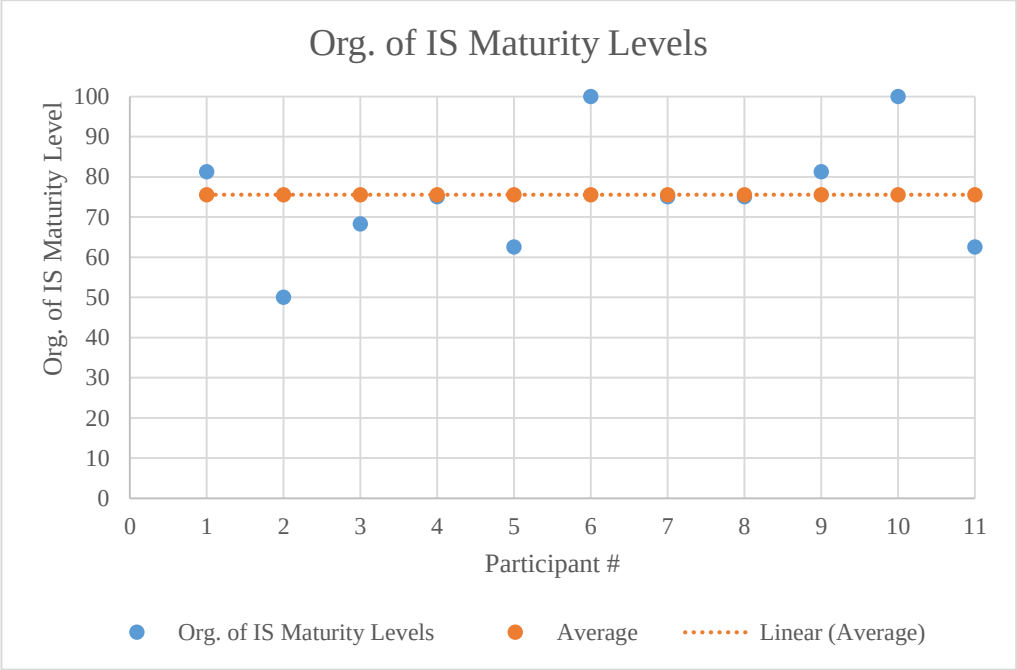


4.2 ORGANIZATION OF INFORMATION SECURITY MATURITY LEVELS (A.6)

According to the answers attendants provided to the questions related to organization of information security controls; reason of the gap between maturity levels of attendants is mainly mobile security policies. Most of the participants (8) has mobile security policies

in place and, some of them (3) has not yet, but they are working on such a policy for their mobile workforce. Visualization of maturity levels can be seen on figure 4-2.

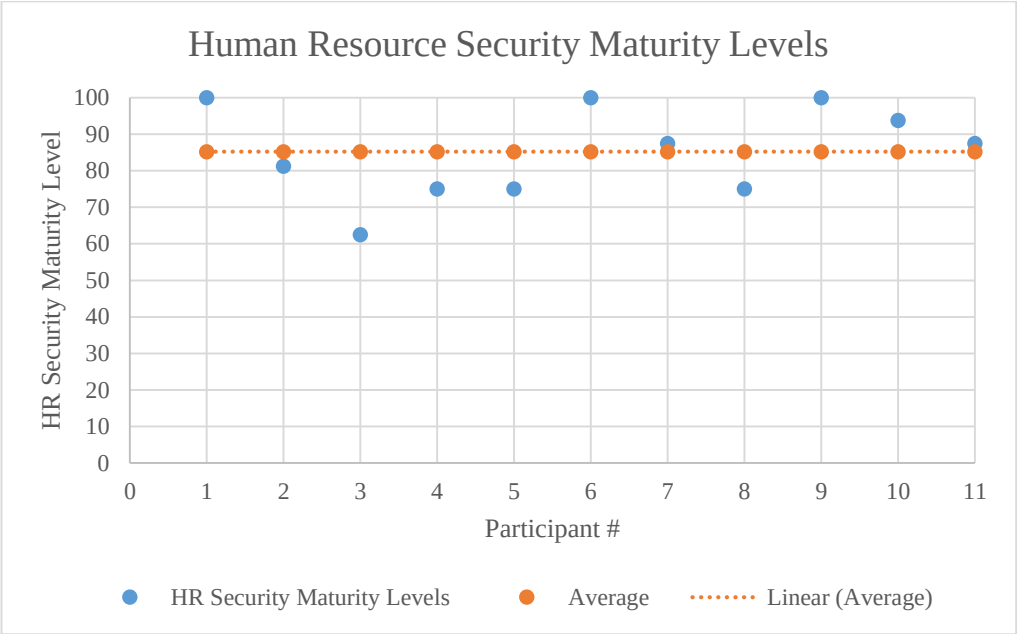
Figure 4-2: Organization of IS Maturity Levels



4.3 HUMAN RESOURCE SECURITY MATURITY LEVELS (A.7)

According to answers given, only one of participants has not a policy for background checks of candidates. As management is aware of that need, there is no such policy in place. All other participants have proper policies in place for both background checking and contractor awareness. Only three of them is reviewed in periodic intervals. Visualization of maturity levels for human resource security can be seen on figure 4-3.

Figure 4-3: Human Resource Security Maturity Levels



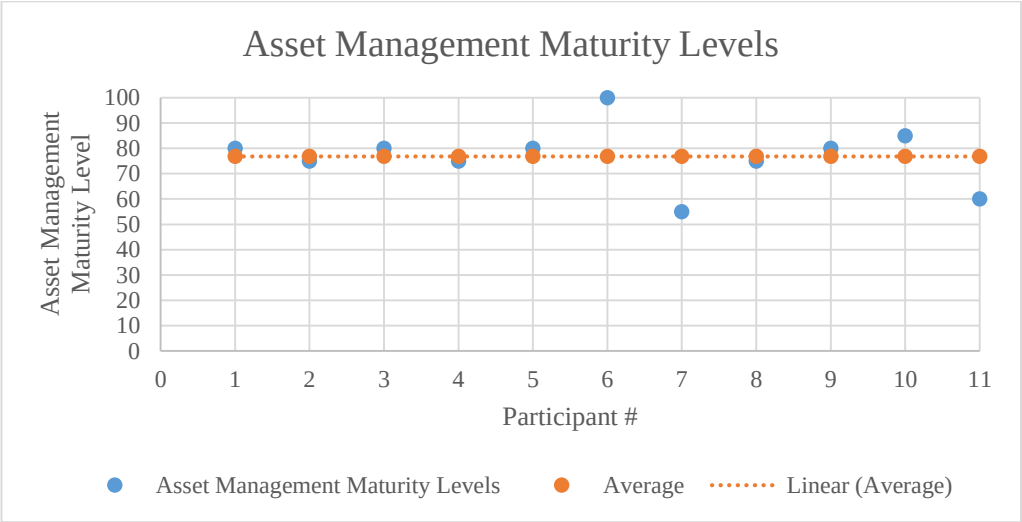
4.4 ASSET MANAGEMENT MATURITY LEVELS (A.8)

Considering the answers provided by participants to questions related to asset management; we can figure out that main differentiation area for maturity level is the acceptable use policy for informational assets which includes the return policy of employees or external parties upon termination of their contract.

Most participants have an acceptable use policy in place, one of them is appropriately reviewing and updating the policy in planned intervals but one of the participants has no such policy or a need for such a policy identified.

Visualization of maturity levels based on answers is shown in figure 4-4.

Figure 4-4: Asset Management Maturity Levels

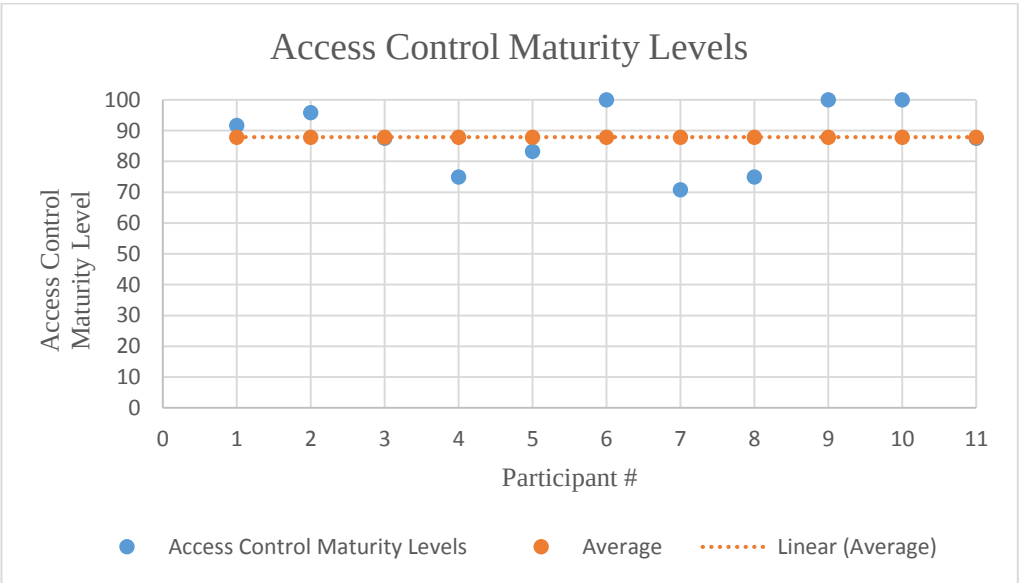


4.5 ACCESS CONTROL MATURITY LEVELS (A.9)

According to the responses collected from participants, every participant has an access control policy based on business needs, there are password rules for identity and access services. Most of them are evaluating the policy document in predefined intervals and upgrading when necessary. Only one participant claimed that they are in progress for developing a policy document so that no review has been made yet.

Maturity levels derived from participants scores is visualized in figure 4-5.

Figure 4-5: Access Control Maturity Levels

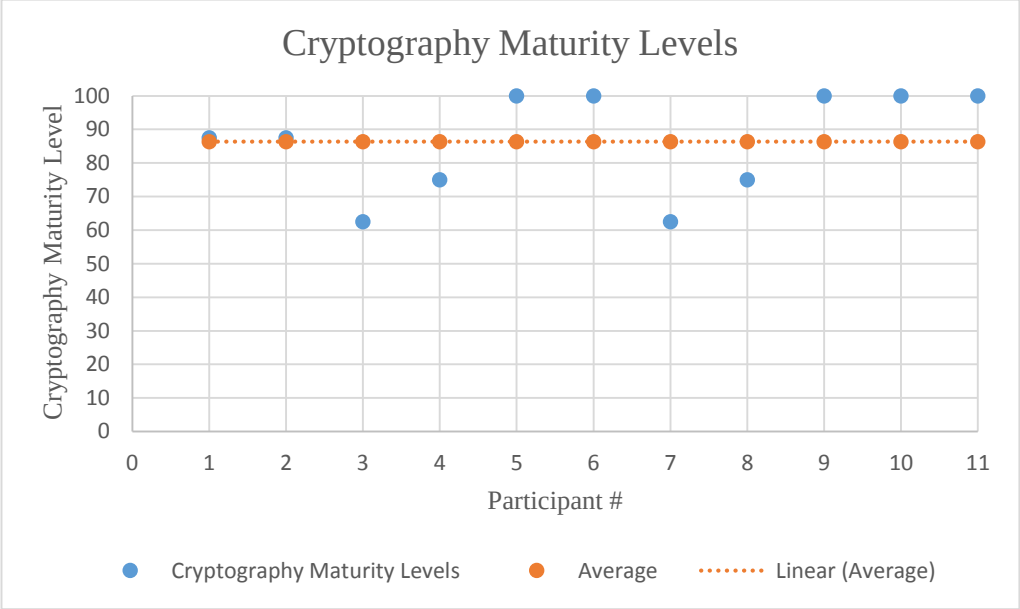


4.6 CRYPTOGRAPHY MATURITY LEVELS (A.10)

Based on the responses to cryptography related questions of survey, every participant has an effective key management system for protecting information assets. Two of eleven participants are in progress for establishing ground rules for cryptographic communication and key management. Other participants have already a policy in place and five of them is continuously reviewing the policies.

Maturity levels for cryptography of participants is visualized in figure 4-6.

Figure 4-6: Cryptography Maturity Levels

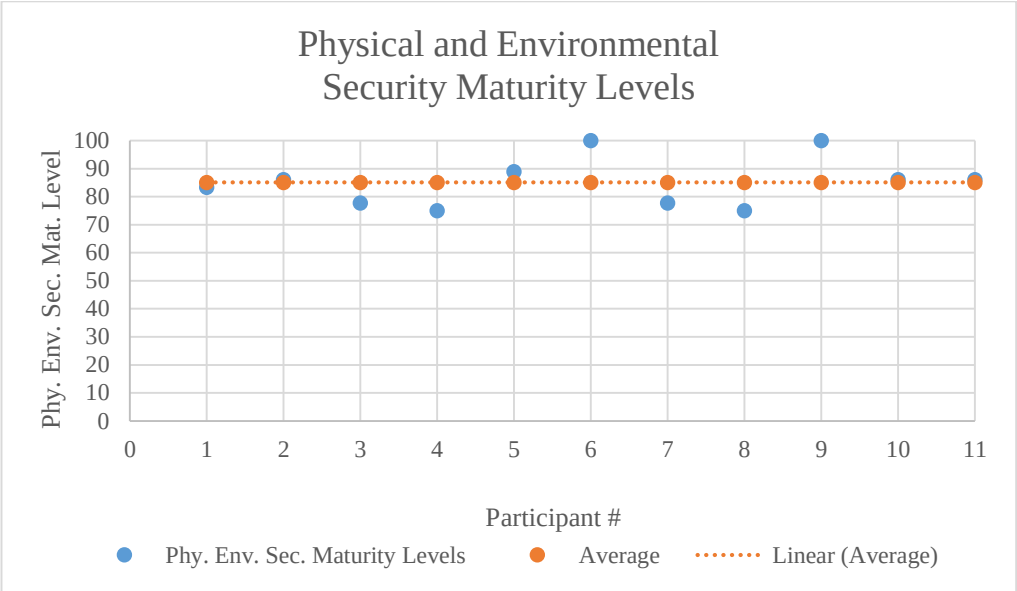


4.7 PHYSICAL AND ENVIRONMENTAL SECURITY MATURITY LEVELS (A.11)

Answers to survey relieved that companies do not review their policies for equipments. Mostly they set the policies but do not review from time to time. Also other some of the companies is in progress for developing policies for taking equipment off-site and security for delivery and loading sections in facilities. Also most important result is one of the attendants has no clear desk policy in place. It will be developed soon.

Scores for maturity levels based on responses from attendants can be seen on figure 4-7.

Figure 4-7: Physical and Environmental Security Maturity Levels

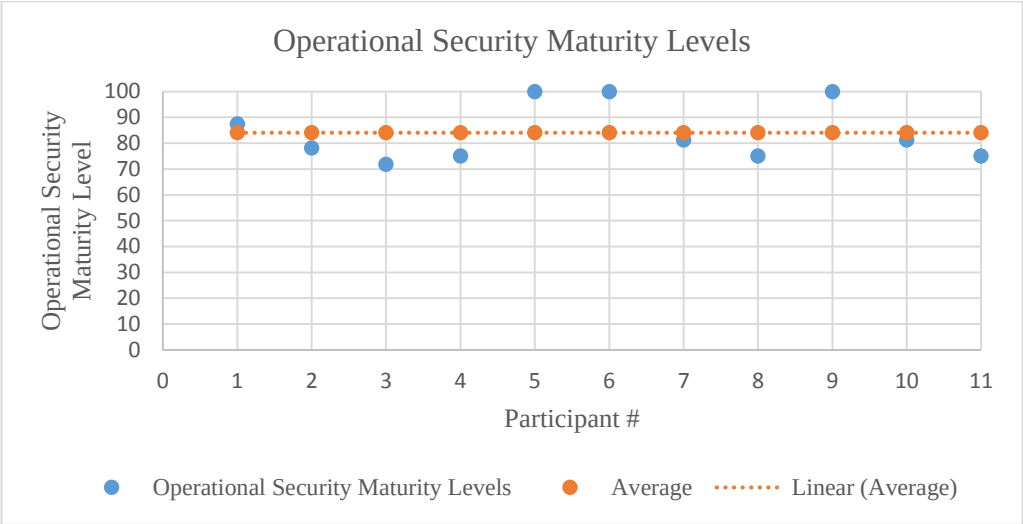


4.8 OPERATIONS SECURITY MATURITY LEVELS (A.12)

When we check the answers for operational procedures and responsibilities section (A.12) we see that the most weak section is about obtaining information about technical vulnerabilities of information systems being used in a timely fashion. Three of eleven attendants are in progress for setting up a policy to obtain information of technical vulnerabilities.

Other source of pain is to restrict the installation of software to production systems. Mostly this is one of the improvement area for information security management. Responses from attendants is visualized in figure 4-8.

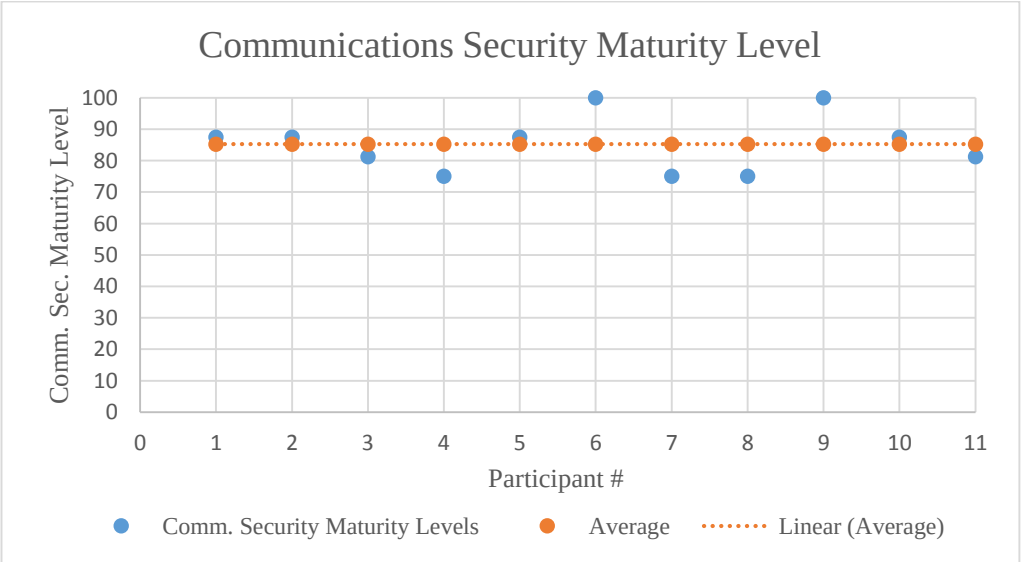
Figure 4-8: Operational Security Maturity Levels



4.9 COMMUNICATIONS SECURITY MATURITY LEVELS (A.13)

When looking at the communications security section; main area for gap is identification of security mechanisms and management requirements of all network services is and inclusion in service agreements. Most of the participants have a policy about identification but this is not reviewed properly. Also another reason for gap between participants is having formal transfer policies and procedures in place. Some of the attendants are in progress for implementing a policy while others have some; but not reviewed regularly. Scores from responses to related questions is shown in figure 4-9.

Figure 4-9: Communications Security Maturity Levels



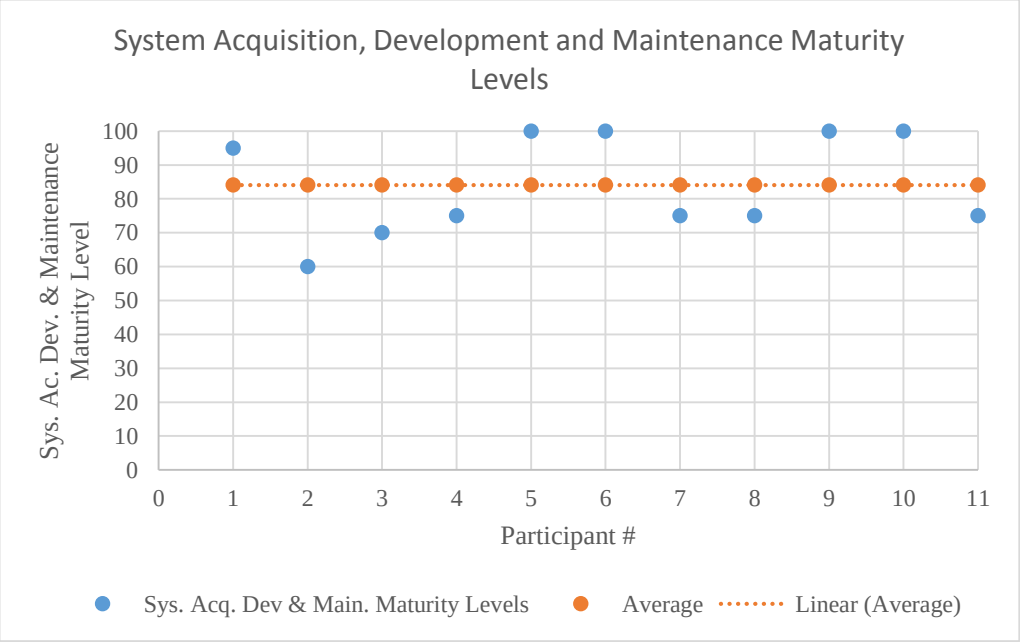
4.10 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE MATURITY LEVELS (A.14)

When looking at the results from system acquisition, development and maintenance section we can easily divide attendants in two major parts. Ones with proper policies and proper review schedule; and ones that have policies but no review.

There are two participants that are in progress for developing a policy for supervising the outsourced system development and rules for rules for development, change management and restrictions during development lifecycle of software and systems in a secure manner.

Visualized results for system acquisition, development and maintenance category can be seen on figure 4–10.

Figure 4-10: System Acquisition, Development and Maintenance Maturity Levels

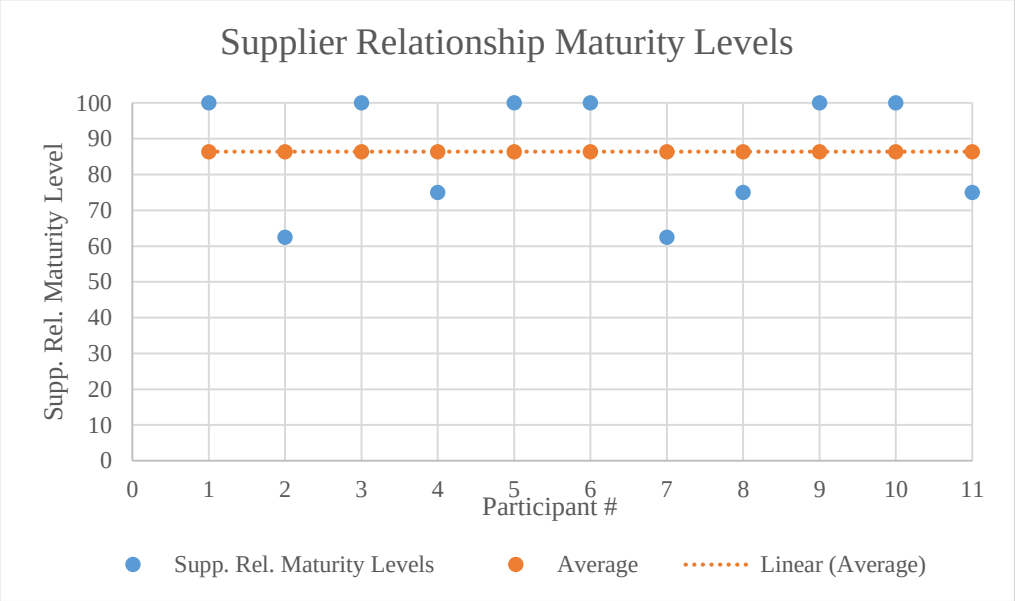


4.11 SUPPLIER RELATIONSHIP MATURITY LEVELS (A.15)

The results for supplier relationship section (A.15) shows the maturity levels for protection of the organizations assets that is accessible for suppliers. As shown in figure 4-11, there are two major groups of attendants.

Six over eleven of them has proper policies with proper review schedules but five of eleven does not review even there is a policy in place. Two of those five is in progress for implementing a policy but this process has not finished yet.

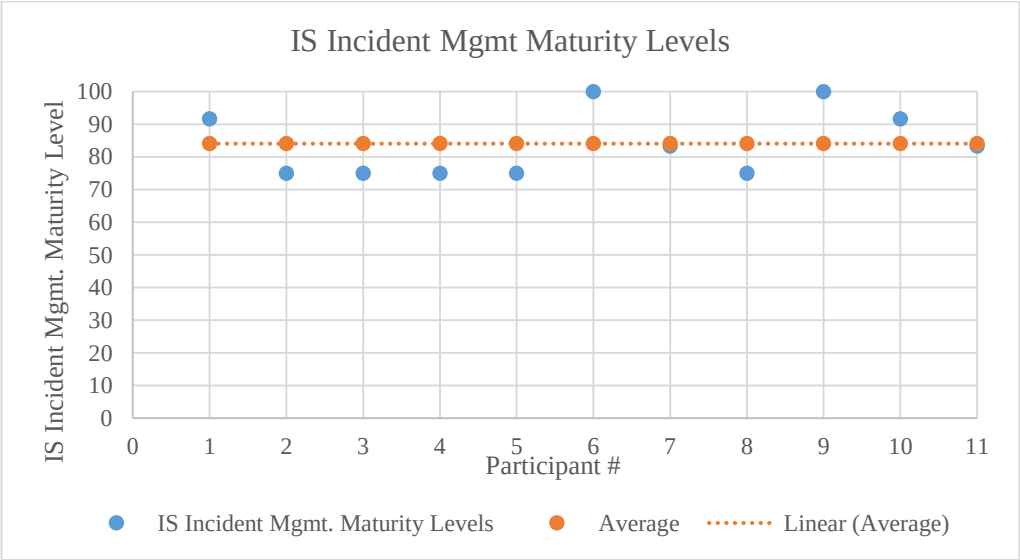
Figure 4-11: Supplier Relationship Maturity Levels



4.12 IS INCIDENT MANAGEMENT MATURITY LEVELS (A.16)

Information security incident management maturity level comparison between participants shows us that every participant has an information security incident management policy or proper procedures in place but two of them are reviewed properly as shown in figure 4-12. Only one participant is in process for establishing management responsibilities and procedures to ensure a quick and effective response to information security incidents.

Figure 4-12: IS Incident Management Maturity Levels



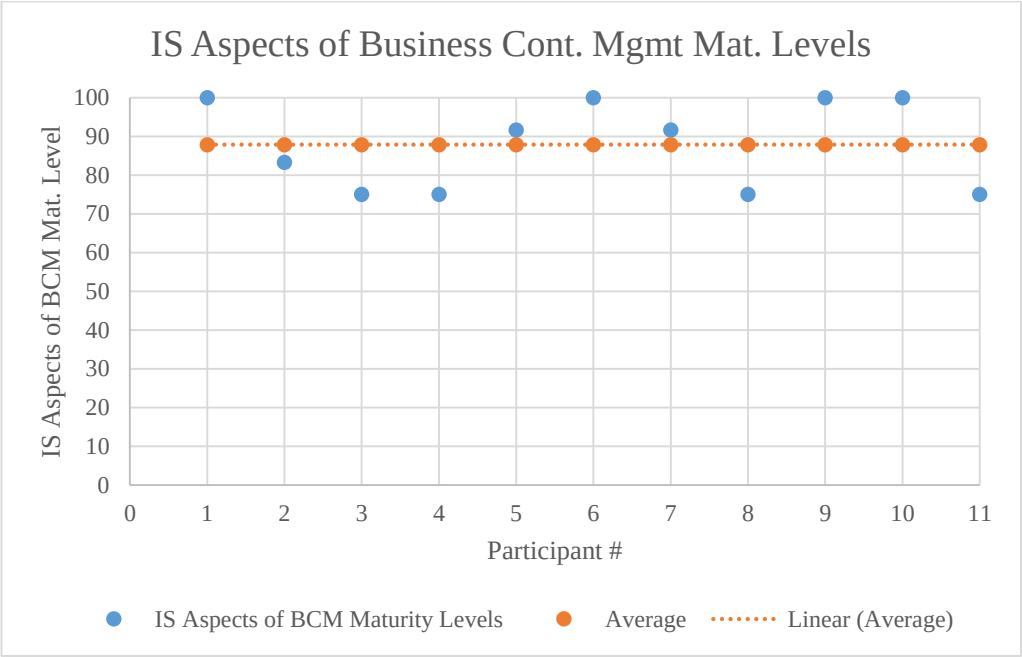
4.13 IS ASPECTS OF BUSINESS CONTINUITY MANAGEMENT MATURITY LEVELS (A.17)

Results for questions in information security aspects of business continuity management section shown in figure 4-13 shows that participants are divided into two major categories. Most differentiated question within the section is "Organization verifies the established and implemented information security continuity controls at regular intervals for ensuring they are valid and effective." Five of eleven attendants has a policy or procedure in place for ensuring the effectiveness of established information security continuity controls at regular intervals which is reviewed properly.

Five of eleven has a policy about ensuring effectiveness, but this policy or procedure is not reviewed properly. One of eleven attandants is in process for developing a procedure for controlling effectiveness of established and implemented information security continuity controls.

Another factor creating the gap between two group of attendants is planning, establishing and maintaining of organizational requirements for information security and continuity of information security management.

Figure 4-13: IS Aspects of Business Continuity Management Maturity Levels

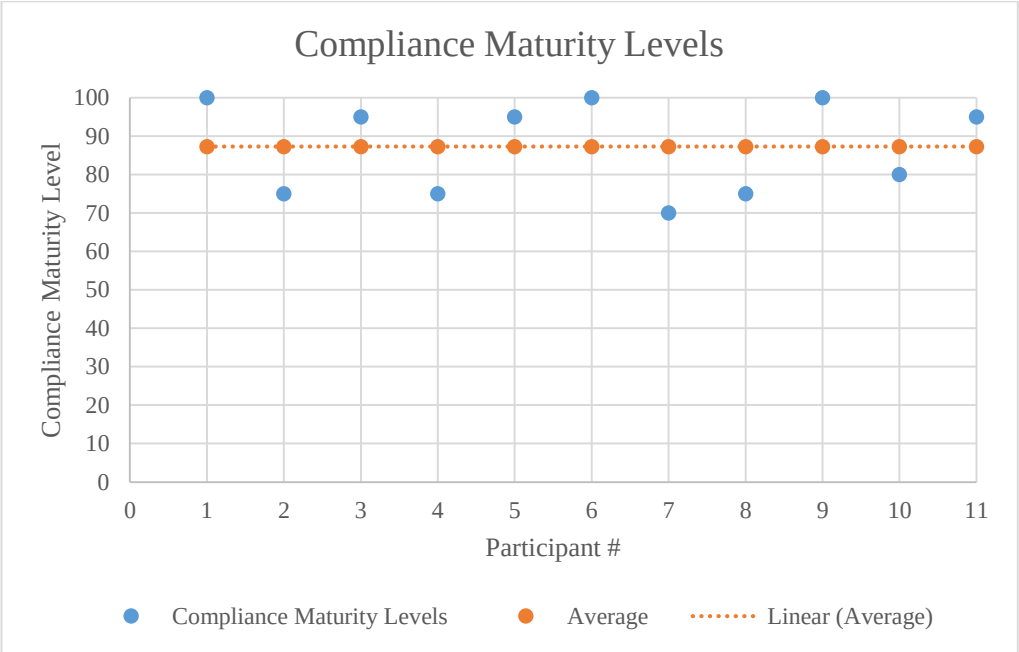


4.14 COMPLIANCE MATURITY LEVELS (A.18)

Maturity scores derived from answers to compliance section divides the attendants in two groups. Six of eleven is with a score of greater than ninety while five of eleven is lower than eighty.

Main reason for that difference is lack of implementation of appropriate procedures to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights. Three attendants from those five who are below eighty either has not started any policy or procedures, or have not finished yet. Visualization of results can be seen on figure 4-14.

Figure 4-14: Compliance Maturity Levels



4.15 OVERALL ISO 27001:2013 MATURITY LEVELS

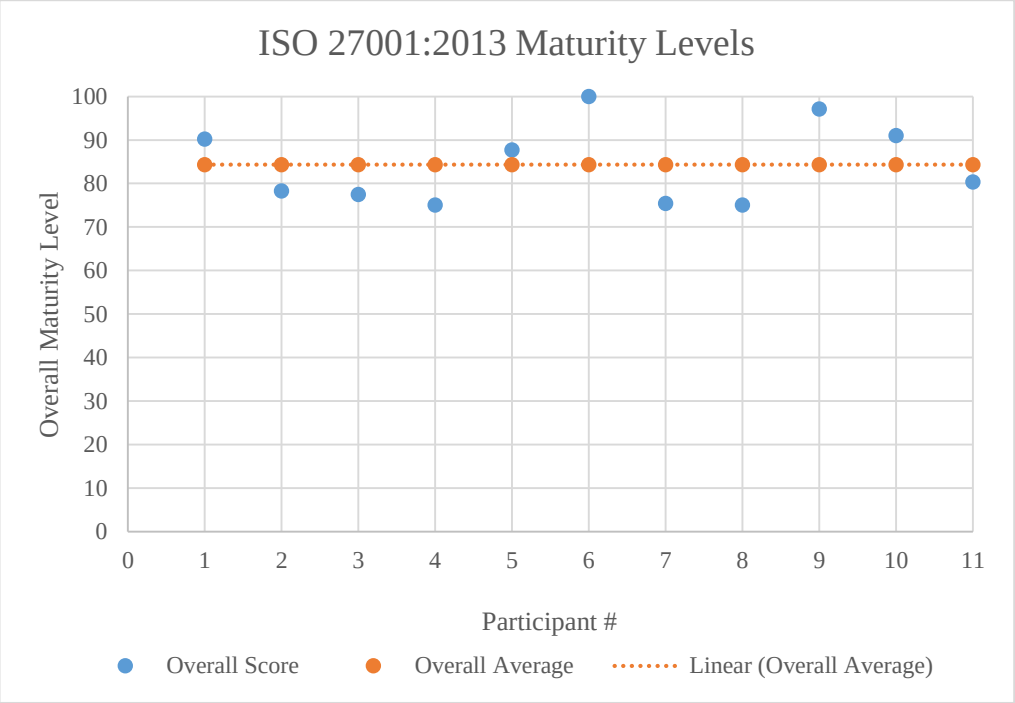
Average scores of each participant for the conducted survey divided by total maximum avilable score of 244 gives the percentage of maturity level for participants. As shown in figure 4-15, there is only one % 100 score. That full score comes from a multi-national bank, whose information security implementation is managed by their foreign shareholders.

Other scores over average of % 84,314 comes from four different financial institutions. Two of them are banks with foreign investors, one of them belongs to a long standing group of companies in Turkey. Last one over average does its business in highly commercial segment. They do not have instruments like personal savings account etc.

Six companies below the average of % 84,314 are mainly banks that are either newly founded and in growing state (both organic and via acquisitions). Some of them did no information on necessity of periodic reviews and thought themselves were “mature enough” and during sessions for this research, found their weaknesses. Those companies below average are at least % 75. We can assume that regulations affecting those

institutions in finance sector leads to % 75 maturity based on this criteria as the regulations must be fulfilled by all the companies in Turkey finance sector.

Figure 4-15: ISO 27001:2013 Maturity Levels



4.16 HOW TO INCREASE OVERALL COMPLIANCE LEVEL

Considering maturity levels listed in Table 4.1: Information Security Management System Maturity Levels; first step is being aware of necessary control. As there is an awareness, there can be a countermeasure rule for mitigating the issue. Without an awareness, there can not be any countermeasures; thus we can not think about a maturity level. (0 %)

Management support is another key in implementing information security management system, thus having a higher maturity level of 25 %.

As application of necessary controls are establihed within the scope of information security management system, maturity level also increases from 50 % to 75 % for given control.

Reviewing the controls is the critcal action in increasing the maturity level. When reviews or controls made in regular basis, maturity levels increase from 75 % to 100 %.

Table 4.1: Information Security Management System Maturity Level

Level	Maturity level in one to five scale
1	**No awareness** about the control or **no countermeasure rules** are established
2	Management is **aware of the control** and **will establish** a rule in the **future.**
3	Necessary **rules and controls are being established** with the approval of management. **But no review has been made.**
4	Necessary **rules and controls are established within the scope** aligned with management leadership. **No review of controls has been made.**
5	Necessary **rules and controls are established** within the scope with management leadership. **Review is made on a regular basis**.

5. CONCLUSION AND RECOMMENDATIONS

5.1 CONCLUSION

The aim of this thessis was to review the maturity levels of organizations in Turkey financial services industry. Also maturity levels of attendants will lead to industry maturity levels by induction. Having these informations in place, companies in finance sector may redirect their investments to their weaknesses.

Firstly, a literature review has been made to clarify terms information, security and information security. For this clarification; different approaches including ITIL, COBIT and ISO/IEC 27001 are detailed.

After clarification of terminology, a survey is conducted among eleven companies in financial services industry. There were 62 clauses in survey which are derived from ISO 27001:2013 standard.

Survey results showed that there are rules, policies or controls established with management authorization or at least approval. On the other hand, there are still some shortages in some control categories like organization of information security section. Only eight of eleven attendants have mobile security policy in place, three of them is in process for developing such policy for their mobile workforce. We can assume that with the spreading need of mobility in the enterprise; every company in financial services industry will have a mobile security policy in place with proper reviews.

While reviewing the overall maturity levels for attendants; results show that the minimum maturity level is % 75. As all the companies in financial services sector should follow the guidance provided by government officials; we can assume that the regulations in Turkey lead to a maturity level of % 75 in ISO/IEC 27001:2013 standard.

5.2 LIMITATIONS

Even tough the survey is conducted with eleven banks in financial services; there were some companies which did not want to participate in this survey. They claimed that they were regulated by COBIT standard and there is no need for an evaluation on ISO 27001:2013 standard.

If the survey is conducted on different subset of companies like retirement or insurance; there may be more comparable and sufficient results.

5.3 IMPLICATIONS FOR FURTHER RESEARCH

Survey was based on clauses and an evaluation criterion. There were no evidence collected from attendants. For supporting the consistency of results and detail of this study; evidences related to questions would be obtained from the organizations participated in research.

This survey - based scoring methodology can be used in different further researchs. Specially when comparison of two or more different subjects is needed.

REFERENCES

Books

Carlson, T., 2001. *Information Security Management: Understanding ISO 17799.* Lucent Technologies Worldwide Services.

OGC, 2013. ITIL v3, Service Design. %1 içinde*Service Design.* basım yeri bilinmiyor:OGC, p. 244.

Simpson, D., 2014. *Transitioning to ISO 27001:2013,* basım yeri bilinmiyor: SAI Global.

Valdevit, T., Mayer, N. & Barafort, B., tarih yok *Tailoring ISO/IEC 27001 for SMEs: A guide to implement an Information Security Management System in small settings.*. Berlin, Heidelberg.

Whitman, M. & Matthord, H. J., 2011. *Principles of Information Security.* Boston: Course Technology.

Periodicals

Beautament, A. & Sasse, A., 2009. The Economics of User Effor in Information Security. *Computer Fraud & Security*, October, pp. 8-12.

Greene, J. R., 2012. The Encyclopedia of Police Science. %1 içinde*The Encyclopedia of Police Science, Third Edition.* New York: Routledge, p. 665.

Pelnekar, C., 2011. *Planning for and Implementing ISO 27001.* [Çevrimiçi] Available at: http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx

Van Niekerk, J. & Von Solms, R., 2010. Information security culture: A management perspective. *Computers & Security*, 30 06.pp. 476-486.

Vural, Y. & Sağıroğlu, Ş., 2007. *Kurumsal Bilgi Güvenliği: Güncel Gelişmeler.*

Other Publications

Association, T. B., 2014. *Banks, branches and Employees of Banks in Turkey.* [Çevrimiçi]
Available at: http://www.tbb.org.tr/en/banks-and-banking-sector-information/statistical-reports/june--2014---banks,-branches-and-employees/980
[Erişildi: 1 September 2014].

Aydoğmuş, E., 2010. *Assessment of Information Security Maturity Levels and ISO/IEC 27001:2005 Compliance of Organizations in Turkey,* Istanbul: İ.T.Ü..

Beautament, A. & Sasse, A., 2009. The Economics of User Effor in Information Security. *Computer Fraud & Security*, October, pp. 8-12.

Business Dictionary, 2013. *What is Information.* [Çevrimiçi]
Available at: http://www.businessdictionary.com/definition/information.html

Carlson, T., 2001. *Information Security Management: Understanding ISO 17799.* basım yeri bilinmiyor:Lucent Technologies Worldwide Services.

Greene, J. R., 2012. The Encyclopedia of Police Science. %1 içinde*The Encyclopedia of Police Science, Third Edition.* New York: Routledge, p. 665.

Kosutic, D., 2014. *iso27001 Standard.* [Çevrimiçi]
Available at: http://blog.iso27001standard.com/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/
[Erişildi: April 2014].

NIST, 2013. *NIST Computer Security Resource Center.* [Çevrimiçi]
Available at: http://csrc.nist.gov

OGC, 2013. ITIL v3, Service Design. %1 içinde*Service Design.* basım yeri bilinmiyor:OGC, p. 244.

Open University, 2013. *Open University, Information Security Management.* [Çevrimiçi]
Available at: http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-0

Pelnekar, C., 2011. *Planning for and Implementing ISO 27001.* [Çevrimiçi]
Available at: http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx

Ramakrishnan, P., 2013. *Information Security Management Systems.* [Çevrimiçi]
Available at: https://www.cccure.org/Documents/ISMS/isms.pdf

Simpson, D., 2014. *Transitioning to ISO 27001:2013,* basım yeri bilinmiyor: SAI Global.

Spreading Science, 2013. *D-I-K-W Model of Innovation.* [Çevrimiçi]
Available at: http://www.spreadingscience.com/our-approach/diffusion-of-innovations-in-a-community/1-the-dikw-model-of-innovation/

Study, B. I. 2. C., 2012. *Brookson.* [Çevrimiçi]
Available at: http://www.brookson.co.uk/documents/case-studies/brookson%20iso%2027001%20case%20study.pdf
[Erişildi: 2014].

the ISO 27000 Directory, 2013. *An Introduction to ISO 27001.* [Çevrimiçi]
Available at: http://www.27000.org/iso-27001.htm

Valdevit, T., Mayer, N. & Barafort, B., tarih yok *Tailoring ISO/IEC 27001 for SMEs: A guide to implement an Information Security Management System in small settings.*. Berlin, Heidelberg.

Van Niekerk, J. & Von Solms, R., 2010. Information security culture: A management perspective. *Computers & Security,* 30 06.pp. 476-486.

Vural, Y. & Sağıroğlu, Ş., 2007. *Kurumsal Bilgi Güvenliği: Güncel Gelişmeler.* basım yeri bilinmiyor, yazarı bilinmiyor

Whitman, M. & Matthord, H. J., 2011. *Principles of Information Security.* Boston: Course Technology.

Zakaria, K., 2009. *Ensuring Information Security Through ISMS,* basım yeri bilinmiyor: Zakaria, Khurram.

APPENDICES

APPENDIX A: ISO/IEC 17799:2005 Clauses and Controls

A.5 Security policy

A.5.1 Information security policy

Management should define a policy to clarify their direction of, and support for, information security, meaning a short, high-level information security policys tatement laying down the key information security directives and mandates for the entire organization. This is normally supported by a comprehensive suite of more detailed corporate information security policies, typically in the form of an information security policy manual. The policy manual in turn is supported by a set of information security standards, procedures and guidelines.

A.6 Organization of information security

A suitable information security governance structure should be designed and implemented.

A.6.1 Internal organization

The organization should have a management framework for information security. Senior management should provide direction and commit their support, for example by approving information security policies. Roles and responsibilities should be defined for the information security function. Other relevant functions should cooperate and coordinate their activities. IT facilities should be authorized. Confidentiality agreements should reflect the organization's needs. Contacts should be established with relevant authorities (e.g. law enforcement) and special interest groups. Information security should be independently reviewed. (Valdevit, et al., tarih yok)

A.6.2 External parties

Information security should not be comprosed by the introduction of third party products or services. Risks should be assessed and mitigated. when dealing with customers and in third party agreements.

A.7 Asset management

The organization should be in a position to understand what information assets it holds, and to manage their security appropriately.

A.7.1 Responsibility for assets

All information assets should be accounted for and have a nominated owner. An inventory of information assets (IT hardware, software, data, system documentation, storage media, supporting assets such as computer room air conditioners and UPSs, and ICT services) should be maintained. The inventory should record ownership and location of the assets, and owners should identify acceptable uses.

A.7.2 Information classification

Information should be classified according to its need for security protection and labelled accordingly.

A.8 Human resources security

The organization should manage system access rights etc. for 'joiners, movers and leavers', and should undertake suitable security awareness, training and educational activities.

A.8.1 Prior to employment

Security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (adequate job descriptions, pre-employment screening) and included in contracts (e.g. terms and conditions of employment and other signed agreements on security roles and responsibilities).

A.8.2 During employment

Management responsibilities regarding information security should be defined. Employees and (if relevant) third party IT users should be made aware, educated and trained in security procedures. A formal disciplinary process is necessary to handle security breaches.

A.8.3 Termination or change of employment

Security aspects of a person's exit from the organization (e.g. the return of corporate assets and removal of access rights) or change of responsibilities should be managed.

A.9 Physical and environmental security

Valuable IT equipment should be physically protected against malicious or accidental damage or loss, overheating, loss of mains power etc.

A.9.1 Secure areas

This section describes the need for concentric layers of physical controls to protect sensitive IT facilities from unauthorized access.

A.9.2 Equipment security

Critical IT equipment, cabling and so on should be protected against physical damage, fire, flood, theft etc., both on- and off-site. Power supplies and cabling should be secured. IT equipment should be maintained properly and disposed of securely.

A.10 Communications and operations management

This lengthy, detailed section of the standard describes security controls for systems and network management.

A.10.1 Operational procedures and responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Duties should be segregated between different people where relevant (e.g. access to development and operational systems should be segregated).

A.10.2 Third party service delivery management

Security requirements should be taken into account in third party service delivery (e.g. IT facilities management or outsourcing), from contractual terms to ongoing monitoring and change management.

A.10.3 System planning and acceptance

Covers IT capacity planning and production acceptance processes.

A.10.4 Protection against malicious and mobile code

Describes the need for anti-malware controls, including user awareness. Security controls for mobile code 'associated with a number of middleware services' are also outlined.

A.10.5 Back-up

Covers routine data backups and rehearsed restoration.

A.10.6 Network security management

Outlines secure network management, network security monitoring and other controls. Also covers security of commercial network services such as private networks and managed firewalls etc.

A.10.7 Media handling

Operating procedures should be defined to protect documents and computer media containing data, system information etc. Disposal of backup media, documents, voice and other recordings, test data etc. should be logged and controlled. Procedures should be defined for securely handling, transporting and storing backup media and system documentation.

A.10.8 Exchange of information

Information exchanges between organizations should be controlled, for example though policies and procedures, and legal agreements. Information exchanges should also comply with applicable legislation. Security procedures and standards should be in place to protect information and physical media in transit, including electronic messaging (e-mail, EDI and IM) and business information systems.

A.10.9 Electronic commerce services

The security implications of e-commerce (online transaction systems) should be evaluated and suitable controls implemented. The integrity and availability of information published online (e.g. on websites) should also be protected.

A.10.10 Monitoring

Covers security event/audit/fault logging and system alarm/alert monitoring to detectunauthorized use. Also covers the need to secure logs and synchronize system clocks.

A.11 Access control

Logical access to IT systems, networks and data must be suitably controlled to prevent unauthorized use. This is another lengthy and detailed section.

A.11.1 Business requirement for access control

The organization's requirements to control access to information assets should beclearly documented in an access control policy, including for example job-related access profiles (role based access control).

A.11.2 User access management

The allocation of access rights to users should be formally controlled through user registration and administration procedures (from initial user registration through to removal of access rights when no longer required), including special restrictions over the allocation of privileges and management of passwords, and regular access rights reviews.

A.11.3 User responsibilities

Users should be made aware of their responsibilities towards maintaining effective access controls e.g. choosing strong passwords and keeping them confidential. Systems and information should be secured when left unattended (e.g. clear desk and clear screen policies).

A.11.4 Network access control

Access to network services should be controlled, both within the organization and between organizations. Policy should be defined and remote users (and possibly equipment) should be suitably authenticated. Remote diagnostic ports should be securely controlled. Information services, users and systems should be segregated into separate logical network domains. Network connections and routine should be controlled where necessary.

A.11.5 Operating system access control

Operating system access control facilities and utilities (such as user authentication with unique user IDs and managed passwords, recording use of privileges and system security alarms) should be used. Access to powerful system utilities should be controlled and inactivity timeouts should be applied.

A.11.6 Application and information access control

Access to and within application systems should be controlled in accordance with a defined access control policy. Particularly sensitive applications may require dedicated (isolated) platforms, and/or additional controls if run on shared platforms.

A.11.7 Mobile computing and teleworking

There should be formal policies covering the secure use of portable PCs, PDAs, cell phones etc., and secure teleworking ("working from home", "road warriors" and other forms of mobile or remote working).

A.12 Information systems acquisition, development and maintenance

Information security must be taken into account in the Systems Development Lifecycle (SDLC) processes for specifying, building/acquiring, testing, implementing and maintaining IT systems.

A.12.1 Security requirements of information systems

Automated and manual security control requirements should be analyzed and fully identified during the requirements stage of the systems development or acquisition process, and incorporated into business cases. Purchased software should be formally tested for security, and any issues risk-assessed.

A.12.2 Correct processing in application systems

Data entry, processing and output validation controls and message authentication should be provided to mitigate the associated integrity risks.

A.12.3 Cryptographic controls

A cryptography policy should be defined, covering roles and responsibilities, digital signatures, non-repudiation, management of keys and digital certificates etc.

A.12.4 Security of system files

Access to system files (both executable programs and source code) and test data should be controlled.

A.12.5 Security in development and support processes

Application system managers should be responsible for controlling access to development project and support environments. Formal change control processes should be applied, including technical reviews. Packaged applications should ideally not be modified. Checks should be made for information leakage for example via covert channels and Trojans if these are a concern. A number of supervisory and monitoring controls are outlined for outsourced development.

A.12.6 Technical vulnerability management

Technical vulnerabilities in systems and applications should be controlled by monitoring for the announcement of relevant security vulnerabilities, and risk assessing and applying relevant security patches promptly.

A.13 Information security incident management

Information security events, incidents and weaknesses (including near-misses) should be promptly reported and properly managed.

A.13.1 Reporting in information security events and weaknesses

An incident reporting/alarm procedure is required, plus the associated response and escalation procedures. There should be a central point of contact, and all employees, contractors etc. should be informed of their incident reporting responsibilities.

A.13.2 Management of information security incidents and improvements

Responsibilities and procedures are required to manage incidents consistently and effectively, to implement continuous improvement (learning the lessons), and to collect forensic evidence.

A.14 Business continuity management

A.14.1 Information security aspects of business continuity management

This section describes the relationship between IT disaster recovery planning, business continuity management and contingency planning, ranging from analysis and documentation through to regular exercising/testing of the plans. These controls are designed to minimize the impact of security incidents that happen despite the preventive controls noted elsewhere in the standard.

A.15 Compliance

A.15.1 Compliance with legal requirements

The organization must comply with applicable legislation such as copyright, data protection, and protection of financial data and other vital records, cryptography restrictions, rules of evidence etc.

A.15.2 Compliance with security policies and standards, and technical

Compliance Managers and system owners must ensure compliance with security policies and standards, for example through regular platform security reviews, penetration tests etc. undertaken by competent testers.

A.15.3 Information systems audit considerations

Audits should be carefully planned to minimize disruption to operational systems. Powerful audit tools/facilities must also be protected against unauthorized use.

APPENDIX B: CHANGES IN ISO/IEC 27001 2013 REVISION

Eleven sections in 2005 edition is increased to 14 sections. Section A.10 Communications and Operations Management is split into two sections: A.12 Operations Security and A.13 Communications Security. Another section is added as A.10 Cryptography. Sections in ISO 27001 2013 edition is listed below:

A.5: Information security policies

A.6: Organization of information security

A.7: Human resource security

A.8: Asset management

A.9: Access control

A.10: Cryptography

A.11: Physical and environmental security

A.12: Operations security

A.13: Communications security

A.14: System acquisition, development and maintenance

A.15: Supplier relationships

A.16: Information security incident management

A.17: Information security aspects of business continuity management

A.18: Compliance; internal requirements like policies, and with external requirements, such as laws

There are new controls added to standard in 2013 revision.

A. 6.1.5 Information security in project management

A.12.6.2 Restrictions in software installation

A.14.2.1 Secure development policy

A.14.2.5 Secure system engineering principles

A.14.2.8 System security testing

A.15.1.1 Information security policy for supplier relationships

A.15.1.3 Information and communication supply chain

A.16.1.4 Assessment and decision on information systems

A.16.1.5 Response to information security incidents

A.17.2.1 Availability of information processing facilities

APPENDIX C: Table 3.2: Information Security Survey Questions and Related Control Categories

Statement	Cont. Cat.
There is a defined policy in place, approved by management and reviewed by authorities in planned intervals.	A.5.
Roles and responsibities in information security are defined and segregated properly, communicated with the authorities or other third parties	A.6
Information security is applied in project management?	A.6
There is a policy for mobile devices and managing the risks involved with mobile device usage.	A.6
There is a policy for supporting security measures for protection of information accessed, processed or stored at teleworking sites -	A.6
There is a policy for background checks on candidates for checking with relevant laws and regulations all employees and contractors have proper information on their responsibilities.	A.7
Management requires all employees and contractors to apply information security based on the policies and procedures.	A.7
Employees and contractors receive appropriate information security awareness, education, training and updates on organizational policy changes.	A.7
There is a policy which defines information security responsibilities of employees that remain after termination of employment	A.7
There is an inventory of information assets and information processing facilities with their owners	A.8
There an identified acceptable use policy of informational assets which includes the return policy of employees or external parties upon termination of their contract	A.8
There is an information classification policy in place aligned with legal requirements, value, criticality and sensitivity.	A.8
There is a procedure for information labeling and handling policy based on information classification scheme	A.8
There is a procedure for management of removable media in accordance with classification scheme, also a procedure for phyical transfer and, disposal of media.	A.8
There is an access control policy based on business and information security requirements established, documented and reviewed.	A.9
Users are provided with access to network and network services that they have been specifically authorized to use.	A.9

There is a formal user registration and de-registration process for assigning access rights, user access provisioning and restriction of allocation and use of privileged access rights -	A.9
Asset owners reviews user access rights in intervals and adjust or remove the rights for employees or external parties upon termination of their employment or contract	A.9
Users have unique identifiers follow a best practice for managing passwords like changing in periodic intervals and controlling complexity and access to information and application system is restricted with secure log on procedures.	A.9
Use of priviliged programs and access to program source code is restricted and controlled.	A.9
Company uses an effective key management system for for protecting information assets.	A.10
Company uses cryptographic controls for protecting information assets.	A.10
Security perimeters are defined and used to protect areas that contain sensitive or critical information	A.11
Secure areas are protected by appropriate entry controls for ensuring only authorized personnel are allowed to access	A.11
Physical security for offices rooms and facilities is designed and applied	A.11
Physical protection against natural disasteras or accidents are designed and applied.	A.11
Delivery and loading areas where unauthorized persons could enter is controlled and isolated from information processing areas.	A.11
Power and telecommunication cabling is protected from interception, interference or damage	A.11
Equipment can not be taken off-site without proper authorization –	A.11
Any item containing storage media is verified to ensure that any sensitive data or software has been removed or securely overwritten before disposal or re-use	A.11
There is a clear desk and clear screen policy in place which includes papers and removable storage media.	A.11
There is a documented procedure for change management as well as other operating procedures	A.12
Detection, prevention and recovery controls for protection against malware is implemented with appropriate user awareness	A.12
Backup copies of information, software and system are taken and tested regularly.	A.12
User activities, exceptions, faults and information security events are recorded, kept and reviewed also protected against tampering and unauthorized access.	A.12
System administrator and operator activities are logged and those logs are protected.	A.12
There are restrictions on software installation on operational systems	A.12

Information about technical vulnerabilities of information systems being used is obtained in a timely fashion.	A.12
Audit requirements and activities involving verification of operational systems is carefully planned and aggreed to minimize disruptions on business processes.	A.12
Networks are managed and controlled ro protect information in systems.	A.13
Security mechanisms and management requirements of all network services is identified and included in service aggreements	A.13
There are formal rtansfer policies, procedures and controls in place.	A.13
Requirements in confidentiality or NDA for organization needs for information protection is identified and reviewed regularly.	A.13
There is an explicit requirement document which includes requirements for new information systems or enhancements to existing information systems.	A.14
There are rules for development, change management and restrictions during development lifecycle of software and systems in a secure manner.	A.14
There is a set of rules for supervising the activity of outsurced system development.	A.14
There are system security and acceptance testing procdedures for upgrades and new versions of information systems	A.14
Current data on test environment is selected carefully, protected and controlled.	A.14
There is an agreement on all relevant information security requirements with each suppliers access, process, store the organizations assets which includes risks associated with information and communication technology services.	A.15
Supplier services and changes to the provision of services by suppliers, including maintaining and improving existing information security policies is managed, monitored and reviewed	A.15
Management responsibilities and procedures are established to ensure a quick and effective response to information security incidents.	A.16
Information security events and observed or suspected weaknesses in systems or services noted or reported through appropriate management channels.	A.16
Information security incidents are responded in accordance with documented procedures and knowledge gained from those incidents are used to reduce the likelihood or impact of future incidents. response to information security incidents.	A.16
Organizational requirements for information security and continuity of information security management is planned, established, documented and maintained properly.	A.17
Organization verifies the established and implemented information security continuity controls at regular intervals for ensuring they are valid and effective.	A.17
Information processing facilities are implemented with redundancy to meet availability requirements.	A.17

Appropriate procedures are implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights.	A.18
Records are protected from loss, destruction, falsification unauthorized access and release in acordance with legislatory and regulatory requirements.	A.18
Privacy and protection of personally identifiable information is ensured as required by applicable rules.	A.18
Organizations approach for managing information security and its implementation is reviewed independently at planned intervals.	A.18
Information systems and information processing procedure compliance are reviewed regularly for compliance within the organizations information security policies and standards.	A.18

APPENDIX D: Banks in Turkey Report of The Banks Association of Turkey

Table is derived from BAT Banks, branches and employees report from june 2014. Full report of BAT can be found on statistical reports section of association web site.

	Banka Sayısı	Şube Sayısı	Personel Sayısı
Sektör Toplamı	**46**	**11.137**	**198.894**
Mevduat Bankaları	**33**	**11.096**	**193.552**
Kamu Sermayeli Bankalar	**3**	**3.431**	**53.539**
Türkiye Cumhuriyeti Ziraat Bankası A.Ş.		1.674	24.161
Türkiye Halk Bankası A.Ş.		887	14.487
Türkiye Vakıflar Bankası T.A.O.		870	14.891
Özel Sermayeli Bankalar	**11**	**5.395**	**95.774**
Adabank A.Ş.		1	31
Akbank T.A.Ş.		994	16.365
Anadolubank A.Ş.		114	1.957
Fibabanka A.Ş.		63	1.152
Şekerbank T.A.Ş.		312	4.304
Tekstil Bankası A.Ş.		44	838
Turkish Bank A.Ş.		19	264
Türk Ekonomi Bankası A.Ş.		547	10.084
Türkiye Garanti Bankası A.Ş.		992	19.075
Türkiye İş Bankası A.Ş.		1.341	23.983
Yapı ve Kredi Bankası A.Ş.		968	17.721
Tas.Mevd.Sig. Fon.Devr. Bankalar	**1**	**1**	**227**
Birleşik Fon Bankası A.Ş.		1	227

	Banka Sayısı	Şube Sayısı*	Personel Sayısı
Yabancı Sermayeli Bankalar	**18**	**2.269**	**44.012**
Alternatifbank A.Ş.		73	1.280
Arap Türk Bankası A.Ş.		7	283
Bank Mellat		3	48
Bank of Tokyo-Mitsubishi UFJ Turkey A.Ş.		1	57
Burgan Bank A.Ş.		60	954
Citibank A.Ş.		8	462
Denizbank A.Ş.		709	13.182
Deutsche Bank A.Ş.		1	113
Finans Bank A.Ş.		673	13.759
Habib Bank Limited		1	17
HSBC Bank A.Ş.		311	5.690
ING Bank A.Ş.		327	5.858
Intesa Sanpaolo S.p.A.		1	20
JPMorgan Chase Bank N.A.		1	64
Odea Bank A.Ş.		45	1.282
Société Générale (SA)		16	259
The Royal Bank of Scotland Plc.		1	87
Turkland Bank A.Ş.		31	597
Kalkınma ve Yatırım Bankaları	**13**	**41**	**5.342**
Aktif Yatırım Bankası A.Ş.		8	693
BankPozitif Kredi ve Kalkınma Bankası A.Ş.		1	133
Diler Yatırım Bankası A.Ş.		1	20
GSD Yatırım Bankası A.Ş.		1	26
İller Bankası A.Ş.		19	2.594
İstanbul Takas ve Saklama Bankası A.Ş.		1	255
Merrill Lynch Yatırım Bank A.Ş.		1	46
Nurol Yatırım Bankası A.Ş.		1	36
Standard Chartered Yatırım Bankası Türk A.Ş.		1	31
Taib Yatırımbank A.Ş.		1	29
Türk Eximbank		2	512
Türkiye Kalkınma Bankası A.Ş.		1	651
Türkiye Sınai Kalkınma Bankası A.Ş.		3	316

APPENDIX E: Table 3.4: Information Security Maturity Level Survey in Turkish

Bu çalışma içerisinde yer alan sorular; her bir önermenin kurumunuzdaki olgunluk seviyesine göre işaretlenerek yanıtlanmaktadır. Her bir önerme 1-5 arası olgunluk seviyelerine göre değerlendirilmektedir. Buna göre her bir şık ve ilişkili olgunluk seviyeleri şu şekilde belirlenmiştir:

1. Kurum içerisinde, sözü edilen önerme ile ilgili bir farkındalık yoktur. Dolayısıyla herhangi bir kontrol uygulanmamıştır.
2. Kurum yöneticileri ilgili önerme ile tanımlanan ihtiyacın farkındadır. Ancak gerekli kontroller gelecekte uygulanacaktır.
3. Önerme ile ilgili gerekli kural ve kontroller uygulanmaktadır. Herhangi bir gözden geçirme uygulanmamıştır.
4. Önerme ile ilgili gerekli kural ve kontroller BGYS ölçeği doğrultusunda uygulanmıştır. Herhangi bir gözden geçirme uygulanmamıştır.
5. Önerme ile ilgili gerekli kural ve kontroller BGYS ölçeği doğrultusunda uygulanmıştır. Uygulanan kontroller düzenli olarak gözden geçirilmektedir.

Çalışma içerisinde elde edilen veriler yalnızca akademik amaçlı olarak kullanılmaktadır. Girilen verilerin doğruluğu, finans sektörünün gerçek durumunun ortaya konulabilmesi açısından kritiktir. Elde edilen hiçbir kişisel veri ticari amaçla kullanılmayacak, üçüncü kişi veya kurumlarla paylaşılmayacaktır. Kişisel veriler, yalnızca talebiniz doğrultusunda çalışma sonuçları ile ilgili bilgilendirilmeniz amacıyla toplanmaktadır.

Cümlecik	1	2	3	4	5
Kurum içerisinde tanımlanmış,yönetim tarafından desteklenen ve belirli periyotlarda gözden geçirilen bir bilgi güvenliği politikası yer almaktadır.					
Bilgi güvenliği kapsamındaki görev ve sorumluluklar tanımlanmış ve doğru bir şekilde ayrıştırılmıştır. Bu görev ve sorumlulukların yetkililerle veya diğer üçüncü kişilerle iletişimi gerçekleştirilmiştir.					
Bilgi güvenliği yaklaşımı, proje yönetimine uygulanmıştır.					
Mobil cihazlar ve mobil cihazların kullanımından doğacak risklerin tanımlandığı bir politika yer almaktadır.					
Mobil kullanımın yer aldığı lokasyonlarda erişilen, işlenen veya depolanan verilerin güvenliğini sağlamak için politika yer almaktadır.					

Tüm işe alımlarda veya sözleşmeli çalışmalarda geçerli olmak üzere, kadrolu veya sözleşmeli çalışanların bilgileri dahilinde; adayların geçmişlerinin kurumun tabi olduğu kanunlar ve regülasyonlar doğrultusunda incelenmesini öngören politikalar kullanılmaktadır.					
Yönetim tüm kadrolu ve kontratlı çalışanların bilgi güvenliği politikaları ve prosedürlerine uymalarını zorunlu tutmaktadır.					
Kadrolu ve sözleşmeli çalışanlar bilgi güvenliği politikaları ve bu politikalardaki değişiklikler doğrultusunda zorunlu olarak farkındalık eğitimleri almaktadır.					
Tüm çalışanlar için çalışanların işten ayrılmalarına rağmen geçerli olacak bilgi güvenliği sorumluluklarının belirtildiği politikalar kurum içerisinde yer almaktadır.					
Bilgi varlıkları ve bilgi işlem alanlarının, sahipleri ile birlikte listelendiği bir envanter yer almaktadır.					
Kurum içerisinde bilgi varlıkları ile ilgili olarak çalışanların işten ayrılmaları halinde geri dönüş politikalarını da kapsayan bir kullanım politikası yer almaktadır.					
Kurum içerisinde, kurumun tabi olduğu yasal zorunluluklar paralelinde verilerin sınıflandırılmasını, değerini ve önemini belirleyen politikalar yer almaktadır.					
Kurum içerisinde, bilgi sınıflandırılması politikaları doğrultusunda; bilgilerin tanımlanması ve işlenmesini belirleyen politika ve prosedürler yer almaktadır.					
Kurum içerisinde, bigi sınıflandırılması politikaları doğrultusunda taşınabilir medyaların yönetilmesi, fiziksel olarak transferi ve medyanın yok edilmesine ilişkin politika ve prosedürler yer almaktadır.					
Kurum ve bilgi güvenliği ihtiyaçları doğrultusunda gerçekleştirilmiş, dokümante edilmiş ve düzenli olarak gözden geçirilen bir erişim kontrol politikası mevcuttur.					
Kurum içerisindeki kullanıcılar yalnızca özellikle erişim hakkı sağlandıkları ağ ve ağ kaynaklarına erişebilmektedirler.					
Kurum içerisinde kullanıcı haklarının atanması için, kullanıcı oluşturulması için ve kullanıcılara özel yetkilerin tanımlanması için resmi bir kullanıcı ekleme ve kaldırma prosedürü bulunmaktadır.					
Bilgi varlıklarının sahipleri kullanıcıların varlıklara erişim haklarını düzenli olarak kontrol etmekte ve sözleşme bitişi veya işten ayrılma gibi nedenlerle ilişkisi kesilen kullanıcıların haklarını düzenlemekte veya kaldırmaktadırlar.					
Kullanıcıların kendilerine özel, tekil tanımlayıcıları bulunmaktadır. Kullanıcıların sistemlere erişimi güvenli bir oturum açma altyapısı ile sağlanmaktadır ve kullanıcı parolaları belirli sürelerde değiştirilmek ve çeşitli karmaşıklık kriterlerini karşılamak gibi en iyi uygulamaları karşılamaktadır.					

Yüksek yetki seviyesindeki uygulamalara ve uygulama kaynak kodlarına erişim sınırlandırılmıştır ve kontrol altında tutulmaktadır.					
Kurum, bilgi varlıklarının korunması için aktif bir anahtar değişim algoritması kullanmaktadır.					
Kurum, bilgi varlıklarının korunması için kriptografik kontroller kullanmaktadır.					
Kurum içerisinde hassas ve kritik verilerin bulunduğu alanlara erişim güvenlik alanları ile korunmaktadır.					
Güvenli alanlara giriş; yalnızca yetkilendirilmiş çalışanların girebilmesi için uygun güvenlik kontrolleri ile korunmaktadır.					
Kurum ofisleri, odaları ve tesisleri için fiziksel güvenlik önlemleri tasarlanmış ve uygulanmıştır.					
Doğal felaket veya kazalara karşı güvenliğin sağlanması için fiziksel koruma etkenleri tasarlanmış ve uygulanmıştır.					
Yetkisiz kişilerin giriş riskinin bulunduğu teslimat ve yükleme noktaları bilgi işlem alanlarından izole edilmiştir ve kontrol edilmektedir.					
Güç ve telekomünikasyon kabloları kesinti, parazit ve hasarlara karşı korunmaktadır.					
Ekipmanlar yetkilendirme olmaksızın kurum dışına çıkartılamamaktadır.					
Yeniden kullanım veya yok etme öncesinde, hassas veri veya uygulamaların erişilemez olması için depolama alanı içeren tüm medyalar silinmekte veya güvenli bir şekilde üzerinde yazılmaktadır.					
Kurum içerisinde taşınabilir aygıt ve evrakların dahil olduğu temiz masa ve temiz ekran politikaları kullanılmaktadır.					
Değişiklik yönetimi ve operasyonel işlemler için dokümante edilmiş prosedürler yer almaktadır.					
Zararlı yazılımlara karşı algılama, engelleme ve kurtarma araçları kullanılmakta ve zararlı yazılımlarla ilgili kullanıcı farkındalığı oluşturulmaktadır.					
Bilgi, yazılım ve sistemlerin yedek kopyaları düzenli olarak alınmakta ve test edilmektedir.					
Kullanıcı faaliyetleri, istisnai, hata ve bilgilendirme mesajları kayıt edilmekte, saklanmakta ve yetkisiz erişime veya değiştirilmeye karşı düzenli olarak gözden geçirilmektedir.					
Sistem yöneticisi ve operatör faaliyetleri kayıt altına alınmakta ve bu kayıtlar korunmaktadır.					
Operasyonel sistemler üzerine yazılım yüklenmesi sınırlandırılmıştır.					
Bilgi sistemlerinin teknik zayıflıkları ile ilgili bilgiler kısa sürede elde edilmektedir.					

Aktif sistemlerin kontrolünü gerektiren aktivite ve denetim gereksinimleri iş süreçlerinin en düşük seviyede etkilenmesi için dikkatle planlanmıştır.					
Kurum içerisindeki ağlar, bilgi sistemlerinin korunmasını sağlamak için yönetilmekte ve kontrol altında tutulmaktadır.					
Ağ hizmetleri ile ilgili güvenlik mekanizmaları ve yönetim ihtiyaçları belirlenmiş ve hizmet sözleşmeleri içerisine eklenmiştir.					
Kurum içerisinde resmi transfer politikaları, prosedür veya kontrolleri yer almaktadır.					
Kurumun sahip olduğu bilgi güvenliği ile ilgili gizlilik ihtiyaçları tanımlanmış ve düzenli olarak gözden geçirilmektedir.					
Kurum içinde; içerisinde, yeni oluşturulan bilgi sistemleri veya mevcut bilgi sistemlerine yapılan iyileştirmeler ile ilgili gereksinimlerin de bulunduğu gereksinimler dokümanı bulunmaktadır.					
Kuruma ait yazılım ve sistemlerin yaşam döngüsünün güvenli addedilebilmesi içingeliştirme, değişiklik yönetimi ve sınırlandırma kuralları yer almaktadır.					
Dışkaynak kullanılan sistemlerin geliştirilmesi esnasında uygulanacak kurallar dizisi yer almaktadır.					
Bilgi sistemlerinin yeni sürümleri ve mevcut sürümlere yapılacak güncelleştirmeler için sistem güvenlik ve kabul testleri gerçekleştirilmektedir.					
Test ortamında yer alan veriler dikkatlice seçilmiş, korunmuş ve kontrol altında tutulmaktadır.					
Kurumun birlikte çalıştığı her bir tedarikçi için; tedarikçinin erişim sağladığı, işlediği ve depoladığı bilgi varlıkları ile ilgili olarak, bilgi ve iletişim teknolojileri servisleri ile ilgili risklerin de yer aldığı bilgi güvenliği anlaşması mevcuttur.					
Tedarikçiler ile ilgili mevcut bilgi güvenliği politikarı düzenli olarak incelenmekte ve gözden geçirilmektedir.					
Kurunm içerisinde bilgi güvenliği olaylarına hızlı ve efektif bir tepki verebilmek için yönetim sorumlulukları ve prosedürleri tanımlanmıştır.					
Bilgi güvenliği ile ilgili olaylar ve sistemlerde görülen ya da şüphelenilen zayıflıklar uygun kanallar aracılığıyla raporlanmaktadır.					
Bilgi güvenliği ile ilgili olaylara dokümante edilmiş prosedürler ve önceki olaylardan elde edilen bilgi birikimi ile müdahale edilmekte ve gelecekteki olası bilgi güvenliği olaylarının olasılık veya olumsuz etkilerinin azaltılması sağlanmaktadır.					
Bilgi güvenliği ve bilgi güvenliğinin sürekliliği ile ilgili kurumsal gereksinimler planlanmış, oluşturulmuş, dokümante edilmiş ve düzenli olarak gözden geçirilmektedir.					

Bilgi güvenliği sürekliliği ile ilgili alınmış olan önlem ve kontroller düzenli olarak gözden geçirilmekte ve onaylanmaktadır.					
Bilgi işlem alanları, erişilebilirlik ihtiyacını karşılamak üzere yedekli olarak oluşturulmuştur.					
Yasal ve zorunlu fikri mülkiyet hakları kanunları doğrultusunda uygunluğu sağlamak için gereken prosedürler oluşturulmuştur.					
Kayıtlar; kayıp, değişiklik veya sahtekarlıktan korunmaları maksadıyla yasal zorunluluklar doğrultusunda korunmaktadır.					
Gizlilik ve kişisel veriler ilgili kanun hükümleri doğrultusunda korunmakta ve bu korunma düzenli olarak kontrol edilmektedir.					
Kurumun bilgi güvenliği yönetimi yaklaşımı ve bilgi güvenliği yönetimi implementasyonu bağımsız olarak periyodik olarak kontrol edilmektedir.					
Bilgi sistemleri ve bilgi işlem prosedürlerinin uyumluluğu düzenli olarak kurum bilgi güvenliği yönetim politika ve standartları doğrultusunda kontrol edilmekte ve gözden geçirilmektedir.					