INVESTIGATION OF PUBLIC BROADCASTING CORPORATIONS WITHIN THE FRAMEWORK OF ISO 27001 AND STANDARDS

Şaban GÜRLEYEN

JANUARY, 2021

INVESTIGATION OF PUBLIC BROADCASTING CORPORATIONS WITHIN THE FRAMEWORK OF ISO 27001 AND STANDARDS

BY

ŞABAN GÜRLEYEN

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF ARTS

IN

MANAGEMENT INFORMATION SYSTEMS

Supervisor, Dr. Manu DUBE

YEDITEPE UNIVERSITY

JANUARY, 2021

PLAGIARISM

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

Date:20.01.2021

Name/Surname:

Signature :

ABSTRACT

It aimed to investigate the opinions of the staff of public broadcasting corporations in four continents around the world that have completed ISO27001 Information Security Management System certification processes and put into practice in the research. For this reason, questions asked in the surveys prepared for the relevant units on four different units such as "Management", "Tech Staff", "Information Security Staff" and "Other Staff". Likert scale of five used in the questionnaires that were prepared. Cronbach's Alpha (α) reliability analysis applied to questions in Likert scale. In the findings, the percentages and frequencies are determined and interpreted in order to determine the views of the relevant groups. Because of the findings obtained, it has been determined that the management regards the ISO27001 certification process positively and that it has made a positive contribution in terms of ensuring corporation's processes and information security. In addition, it has observed that the information security team has expressed their opinion that they need the necessary infrastructure, training and staff reinforcement to manage ISO 27001 processes in an active situation. It determined that the Tech Staff gave positive feedback that the ISO 27001 processes facilitated their work and it was important to carry out more work that is efficient but there is no compliance in terms of infrastructure problems and number of staff competencies. It has been determined that all of the unit staff have a positive opinion that awareness training under ISO 27001 is beneficial and that the stages of Information Security Management System are absolutely important for corporate information security.

Keywords: ISO 27001**,** Information Securiy, Information Securiy Standards, Information Security Management, Information Security Systems

ÖZET

Yapılan araştırmada, ISO 27001 Bilgi Güvenliği Yönetim Sistemi sertifika edinim süreçlerini tamamlayıp uygulamaya geçen dünya çapında kamusal yayin yapan yayın kuruluşlarına ait personellerin, oluşturulan sistem hakkındaki gorüşlerinin incelenmesi amaçlanmıştır. Bu nedenle araştırmada, "Yönetim", "Teknik Ekip", "Bilgi Güvenliği Personeli", ve "Diğer Birim Personelleri" gibi dört farklı birimler üzerinde ilgili birimler için hazırlanmış anketlerde, belirli sorular sorulmuştur. Hazırlanmış olan anketlerde, 5'li likert ölçeği kullanılmıştır. Likert ölçeğinde sorularda Cronbach's Alpha (α) güven analizi uygulamaya konulmuştur. Ortaya çıkan bulgularda ilgili grupların görüşlerinin saptanması amacıyla yüzdelik dağılımları ve freakansları saptanarak yorumlanmıştır. Kaydedilen bulgular neticesinde, yönetimin, ISO27001 sertifika edinim sürecine olumlu baktığı, kurumsal süreçlerin ve bilgi güvenliğini sağlaması açısından, olumlu ve önemli bir katkı sağladığı yönünde görüş belirttiği saptanmıştır. Ayrıca, bilgi güvenliği ekibinin, görüşlerinin, ISO27001 süreçlerinin ivedi ve faal bir durumda yönetilebilmesi için gereken altyapısal yeterlilik, personel takviyesi ve eğitim gibi ihtiyaçların olduğu yönünde gözlemlenmiştir. Teknik Ekibin ise, ISO27001 süreçlerinin işlerini rahatlama sağladığı ve daha verimli bir çalışma yürütülmesine olanak verdiği yönünde pozitif geri bildirim verdikleri fakat altyapısal sorunlar ve personel sayısı yeterlilikleri konusunda uyum olmadığı belirlenmiştir. Tüm birim personellerinin, ISO27001 kapsamında alınmış olan farkındalık eğitimlerinin faydalı bulunduğunu ve Bilgi Güvenliği Yönetim Sistemi aşamalarının kurumsal bilgi güvenliği tarafında mutlak önemli olduğu yönünde, olumlu geri bildirim sundukları tespit edilmiştir.

Anahtar Kelimeler: ISO 27001, Bilgi Güvenliği, Bilgi Güvenliği Standartları, Bilgi Güvenliği Yönetimi, Bilgi Güvenliği Sistemleri

ACKNOWLEDGEMENTS

I had support of many people during writing of this thesis.

First, my thesis has dedicated to my brother Mehmet GÜRLEYEN who passed away.

Secondly, I would like to thank my thesis supervisor Dr. Manu Dube, for his guidance and criticism of my work.

I would like to thank all my friends who supported me and never left me alone.

Many thanks to all companies who supported me by answering questions in my survey.

In addition, special thanks to my mom Şükriye GÜRLEYEN and my dad Hulusi GÜRLEYEN who always believed in me about my success in any work I do with all my passion.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

COBIT:	Information and Related Technology Control Goals
DSS:	Data Security Standard
HIPAA:	Health Insurance Portability and Responsibility Act
ISMS:	Information Security Management System
ISO:	International Standard Organization
ISO27001 ISO / IEC 27001:	Information Security Management System Standard
ISO27005 ISO / IEC 27005:	Information Security Risk Management Standard
ITIL:	Information Technologies Infrastructure Library
PCI:	Payment Card Industry
TURKAK:	Turkish Accreditation Agency

1. INTRODUCTION

The concept of information, which gives its name to the age we are in, has been one of the most important elements of the process that has affected production since centuries ago, when humanity has transformed into an information society with technological developments, starting from the Agricultural Society to the industrial society. One of the most important examples of this is the search for knowledge levels and analytical thinking abilities rather than the skills of individuals in businesses. Since information is the most important source of production and provides a competitive advantage to enterprises, it is undoubtedly imperative that enterprises use their information assets in accordance with their purpose and protect them. Especially since the '90s, the need for corporations to protect their information assets has increased as organizations have provided some of their services through this large global network thanks to the internet. Along with attacks on corporate or personal information assets, the importance attached to both personal and corporate information security has increased and has led to the adoption and implementation of new approaches and information security standards within the corporations. Along with attacks on corporate or personal information assets, the importance attached to both personal and corporate information security has increased and has led to the adoption and implementation of new approaches and information security standards within the corporations. (Mete, 2010).

Corporation's information security must provide at each stage of the production, processing, access, and storage of information. For this, software, hardware systems, and human resources that are an indispensable part of information security should take into consideration. In information security approaches where, corporate information assets tried to protected, it accepted that the weakest link of the security chain is always people (Colwill, 2009). The reason for this is that many technical or non-technical security measures implemented incorporate systems that can overcome by attackers in various ways using humans (Arce, 2003).

In order to ensure information security, corporations need to identify and implement a range of security policies and procedures in line with their needs and processes (Asosheh et al., 2013). These policies can reduce to some user processes such as reviewing corporate activities,

monitoring access to the systems, making necessary evaluations by keeping change records, and restricting deletion (Canbek and Sağıroğlu 2006)

In its most basic terms, information security is the process carried out to identify corporate information security risks and to reduce the effects of these risks to acceptable levels. In this context, the adoption of ISMS should be a strategic decision for an organization, because the design and implementation of ISMS directly related to the corporations needs and objectives, security requirements, the processes used, the size and structure of the organization (Asosheh et al., 2013)

Since information security plays a very important role in supporting the activities of the corporation, it is necessary to have a standard or criterion that regulates governance in information security. In order to standardize and streamline information security practices, various standards have been developed to “protect information technology systems and information” by establishing state-owned corporations around the world and by organizations in the private sector (Gikas, 2010).

ISO27001 standard, which is one of these standards, is a standard that made compulsory in many fields every day. Due to its validity within many standards created in the field of information security in the world and its flexible structure applicable to any corporation or organization with its sector independent structure. ISO27001 offers an approach that can effectively manage information security and measure its effectiveness with the help of a number of controls that have been determined in accordance with corporate processes (Rhodes-Ousley, 2013).

Turkey in the context of cyber security and published studies in the field of information security "2016 - 2019 National Cyber Security Strategy and Action Plan" has gained speed. Within the scope of these studies, it requested to establish ISMS (Information Security Management Systems) of public corporations and to establish a sustainable and continuously developable dynamic structure with the ISO27001 certificate of established Information Security Management Systems. Especially in the establishment of KamuNet network, which called as a secure line, where communication provided between public corporations, establishment of ISO27001 has made compulsory for all public corporations (UDHB 2017).

Purpose of Research

ISO27001 ISMS certification brought the public broadcasting corporations and establish corporations with the introduction of the requirement based in Europe, (Turkey, Germany, United Kingdom) America, (USA, Canada, Mexico) Asia, (Qatar, Japan, South Korea) Ocenia, (Australia, New Zealand) with the standard ISO27001. ISO27001 Information Security certification corporations in the process of obtaining public broadcasters and operation of the public-broadcasting corporations were to investigate the applicability of the management system. The sub-objectives determined within the scope of this objective are as follows.

Regarding the applicability of ISO27001 Information Security Management Systems standard in corporations:

1. What are the views of people who have completed the ISO/IEC certification process and are in the Management Level who are in charge of public broadcasting corporations that have active information security?

2. What are the views of the members of the information security team who are responsible for the establishment and effective management of the corporate information security and who employed by the Management in public broadcasting corporations?

3. What are the views of other Tech staff who are indirectly responsible for information security, apart from membership of the Information Security team in public broadcasting corporations that own ISO 27001?

4. What are the views of other staff in corporations that have completed the ISO 27001 certification process and are effectively running information security?

Importance of Research;

Establishing a corporate information security, ensuring the continuity of the established site, continuously monitoring and identifying the adverse aspects of making improvements, creating information security awareness, in short, establishing a live information security is a must for having ISO 27001 certificate. This study sheds light on the effectiveness levels, ownership status

and technical competence of ISMS (Information Security Systems Management) established by public broadcasting corporations.

Assumptions in Research;

It assumed that the staff in the corporations participating in the research have fulfilled the requirements of the ISO27001 processes in their corporations. For example, it is assumed that the senior management and management level reveals the ownership and will that expected of them, that the information security staffs are actively involved in ISO27001 compliance processes and that the staff and technical staff of the corporation reach a certain maturity level by participating in ISO27001 awareness trainings.

Scope and limitations of Research;

The public broadcasting corporations and organizations that broadcast internationally in Turkey and other countries determine the scope. Because the research topic consists of corporate's information security and questions posed to the staff of the corporation in various respects, negative feedback has received from many public broadcasting corporations to the request for the implementation of surveys.

For this reason, the survey work is limited to public broadcasting corporations based in Europe (Turkey, Germany, United Kingdom) America (USA, Canada, Mexico) Asia (Qatar, Japan, South Korea) Ocenia (Australia, New Zealand) that four continents who have received permission, provided their names kept secret. It has observed that the staff in the aforementioned broadcasting company did not participate fully in the survey application.

2. FUNDAMENTAL OF INFORMATION

Information is the level of phenomenon that the human mind can reach the thought that occurs because of the study of intelligence, the thoughts that the mind understands are the whole, and it seems that defined as the meaning obtained from the data. (TDK 2020).

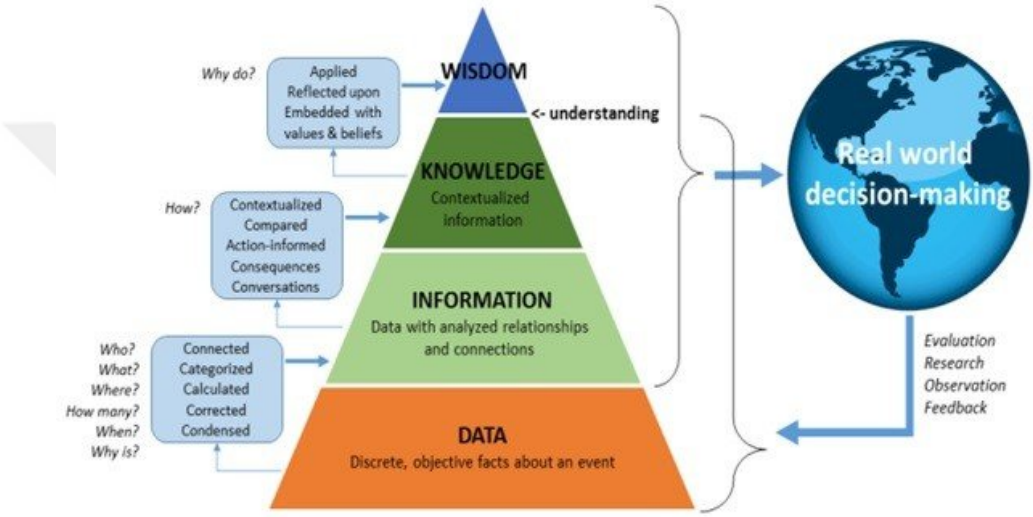

Figure 2. 1 Transition from Data to Wisdom (Bours, 2015)

Knowledge is one of the basic building blocks of perception in the world. Since the beginning of time, man has interpreted his environment effectively, and his ability to understand and use knowledge can seen as man's greatest achievement (Hilton, 2001). Information continues to transfer to various methods of use since the beginning of time.

At first, oral transmissions, stories, fairy tales used. In the following process, educational corporations and books played an important role in the transfer of knowledge. In the recent period, the production, management and sharing of information has become quite easy with the developments in Information Technologies. Processing, transporting and storing information in electronic media allows access to information from any place at any time. Information can also define as data that processed in a certain order, which used to shape future decisions and to make current decisions. If data affects behavior, it can express as information. Information may not always be meaningful. Information that plays an important role in making a particular decision

can only be data at the point of making another decision. At this point, criteria such as reliability of information, how relevant it is to the subject, its completeness, ease of access, meeting the needs determine the quality of its knowledge (Demirtaş, 2013).

The importance of knowledge continues to increase with each passing day. More information is an important tool for you to better adapt to the world around you. In corporations or organizations, information is often one of the most important assets owned by a company. We can also think of information as advantage that separates companies and helps one to be more successful than the other (Rhodes-Ousley, 2013).

2.1.Fundamentals of Information Security

In this section, the definitions necessary to have basic knowledge about information security and its components are given. In order to ensure the security of information, it is necessary to consider the concept of information and the basic elements that directly related to the security of this information.

Information can divide into different categories, such as Table 1.1, moving from unclassified information that is visible to everyone to confidential information that only the most trusted people can access. Depending on the importance, sensitivity and vulnerability of information to theft or abuse, protection needed to control access through different means.

To understand how to secure information assets, you first need to know what that really means. In the most vulgar way, it can express as preventing malevolent people from accessing information that should not be accessible. However, information is only useful if you know it is useful and have access to it. Protecting privacy alone does not mean security assured. In order for a corporation to secure its information, it needs to approach the problem from a human, process and technology perspective (Governence, I. 2019).

Table 2. 1 Information Privacy classes (Governence, I. 2019)

Class	Description
Top Secret	When obtained, it is confidential information that can have a serious impact on reputation, legal status, strategic plans or commercial status. It is accessible only to people who need to know.
Secret	It is information that contains confidential information and new thoughts about future products, plans and processes. The entire collaboration team developing the new plans is entitled to access these documents.
Confidential	Refers to information about existing products, plans, processes and other specific issues. All professional staff are entitled to access.
Restricted	Extended refers to lightly sensitive information for controlled use within the company. However, it is not public information.
Unclassified	Refers to information that freely shared within and outside the company.

In the simplest sense, a technology needs a person to manage and maintain it, and that person needs to monitor defined processes in doing so. This is part of the systematic rendering of Information Security (Governence, I. 2019) Information security is the protection of classified corporate information assets against unauthorized use, access, disclosure, harm, alteration or destruction.

Information security is the process of identifying corporate information security risks and reducing the effects of these risks to acceptable levels (Asosheh et al., 2013).

2.1.1. Key Elements of Information Security

Although information security is said to be based on three basic concepts: privacy, integrity and accessibility, it has been seen that there are many elements as well as these three elements. These elements seen in figure 2.2.

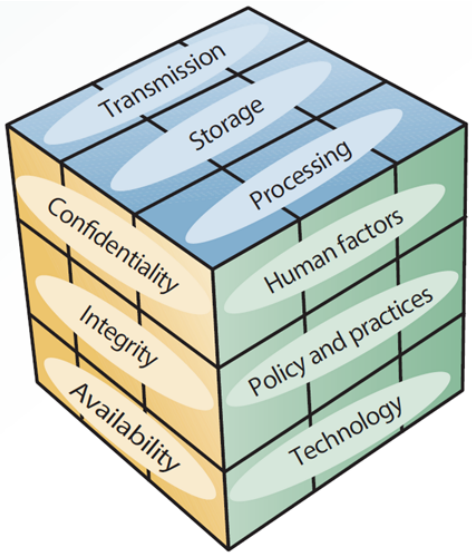

Figure 2. 2 Elements of Information Security (Başaranoğlu, 2016)

Privacy, it refers to the blocking of access to information other than those authorized to exist. The information must be restricted to unauthorized access while it is on computer systems, when it transmitted between systems, and where it is stored.

Integrity, also, it can be expressed as data integrity. It means ensuring that the content of the information asset is protected as it should be or maintained unaltered. For this purpose, data access controls and backup operations must perform periodically.

Accessibility, means ensuring that people with authority can reached now when the presence of information needed. In other words, to ensure that the ISMS carry out the work that expected of them (Kılıç, M.Ç. ve Gökçöl O. 2010)

Information security management, on the other hand, can characterized as a state of balance between the protection of information and its secure access. To ensure this, businesses conduct a

security management within a framework supported by senior management, whose boundaries drawn by various policies.

2.2.Information Security Management System

Providing information security in corporations is not only possible with technology. The perception that technological solutions will suffice is a false perception. Information security is a concept in which technology, process and human factors must evaluated together and created according to these three factors. ISMS at this point is a system built according to technology process human factors. Information security management system; information assets confidentiality, integrity and accessibility of systematic principles, rules laid down, Planned, managed, sustainable, documented and supported valuation accepted international safety standards as the basis of the totality of activities is called. In other words, The Information Security Management System (ISMS) is a framework that enables organizations to manage security events in a holistic and systematic manner. At the same time, ISMS is a system of processes, technology and people that helps manage, monitor, audit and improve the organization's information security.

Within ISMS, it includes human resources, corporate policies, procedures, as well as software and hardware assets as part of the technology. An organization implementing ISMS can protect its information assets against various information security threats. On the other hand, an important part of ISMS is risk management. Risk management is the process by which steps taken to identify, assess and then process risk, reducing it to an acceptable level or eliminating it altogether. While risk assessment carried out, potential risks and weaknesses should identify in accordance with the basic principles of confidentiality, integrity and accessibility. Proper management of ISMS will help the agency to accurately reduce risks and recognize the appropriate control to manage. It will also minimize material losses and impacts during a disaster event. It can also significantly improve the corporation’s perspective on information security management. It can increase information security awareness in all components of the organization (Achmadi et al., 2018).

2.2.1. Types of Information Security Management System

Various ISMS accepted in the world and in Turkey, with the aim of ensuring information security both at the general level and in specific areas. The most widely accepted and widely applied of these:

- COBIT
- HIPAA
- ISO27001
- ITIL
- PCI-DSS

The ISO27001 standard, which is the most widely used in Turkey and is the basis for the main subject of this thesis, will be included more broadly.

PCI-DSS has developed to ensure the security of card payments and to develop an effective protection against counterfeiting and fraud. It is among the standards accepted worldwide. Payment Card Data Security standard is an acronym for PCI DSS, the Turkish equivalent of payment card data security industry.

PCI-DSS consists of six main criteria. There are more than 200 controls based on 12 sub-criteria under these main criteria. The PCI-DSS standard includes all banks that produce cards, all points of sale that accept payments with cards, and all service providers that provide and store data during shopping (Gülmüş, 2010). With PCI-DSS compliance, interested parties will take the necessary precautions to minimize the risks of security breaches. It enables all parties to operate safely, contributes to the development of customer relations, positively affects profit rates and helps to prevent high fines. It positively affects the image of the organization.

COBIT, addresses the need for management and control of information and related information technology (IT). It stands for Control objects for Information and related Technology. It developed by ISACA (Information Systems Audit and Control Association) and ITGI (IT Governance Institute) to set out the goals that need to be achieved in Information Technology Management and its first version published in 1996 (ISACA 2019).

It is a framework for the management of corporate information and technology for the entire enterprise. COBIT identifies components and design factors to create and maintain an optimal management system. It recognizes that effective management of information and Information Technologies is critical to the success and survival of organizations (Lainhart, 2000)

ITIL expressed as a library compiled from best practices used by organizations around the world. It takes its name from the first letters of Information Technology Infrastructure Library, which means Information Technology Infrastructure Library. For enterprise structures, focused on processes and how processes work together to deliver excellent IT services.

Therefore, they also called best practices that support planning, monitoring, and controlling IT services. ITIL provides a clear view of IT operations such as IT management and Event Management, problem Management, Change Management, Configuration Management and availability management (Raflesia et al., 2017)

It originated in the 1980s because of work by the UK Department of Commerce to standardize IT infrastructure and service processes. The most recent release of ITIL is ITIL 3.0, released in 2007. ITIL has become the accepted standard in the world today.

The stages of the ITIL life cycle are:

- Service strategy
- Service Design
- Service transition
- Service process

Continuous service development:

Figure 2. 3 ITIL Lifecycle Stages

Each stage of the ITIL life cycle, as shown in figure 3.2, has different processes in itself. This process should occur under circumstances in which Planned Giving services, which planned to evaluated in terms of the service given to all phases of project management such as how to plan studies. At the same time, how a service that is in the intellectual stage can transferred to live life, the management stages of the service and the determination of the frequency of review are among the activities within the scope of these processes.

HIPAA is a United States legislation that provides rules and regulations to ensure the security of electronic medical records in order to protect the patient's medical privacy. The legislation consists of multiple titles. However, Act II. Its title concerns regulations on the protection and dissemination of transactions of health records. II. Under the title, HIPAA's privacy rule defines national standards for protecting patients ' privacy. In fact, the rule prohibits health professionals from giving the patient's medical data to third parties without explicit written permission from the patient concerned.

Figure 2. 4 HIPAA Compliance Processes (Al-Aqeeli et al., 2017)

Furthermore, access to the patient's medical records without a legitimate reason should not allowed as it violates the patient's privacy. However, where access to the patient's stored medical data is required to further existing medical treatment, HIPAA allows medical professionals to access those records. Finally, penalties and fines for violating the privacy rules set out in the law are disclosed (Al-Aqeeli et al., 2017). HIPAA compliance processes given in the corresponding visual figure 1.4.

3. DESCRIPTION AND IMPLEMENTATION OF ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

3.1. ISO 27000 Family, History and Concepts

In this Section, information security and business continuity phase, people, processes and information assets, ISO27001 management system contains detailed information about have been given.

ISO, (International Organization for Standardization), delegates from 25 countries, began with a meeting in London in 1946 at the Institute of civil engineers and industrial coordination and to facilitate the incorporation of industry standards it decided to create a new international organization. On February 23, 1947, the new organization of ISO officially became operational.

Since its inception, more than 21616 international standards covering nearly all aspects of technology and manufacturing have published. Today, it has members from 163 countries and 779 technical authorities in order to develop standards (ISO 2020)

ISO / IEC 27000 family, standards have been established for the purpose of ensuring organizations have information assets. Using this family of standards helps organizations manage the security of assets such as financial information, intellectual property rights, employee information, or third-party information. ISO27001 Information security management system is the best-known standard of this family. The relationship between the ISO / IEC 27000 standard family shown in Figure 2.1.

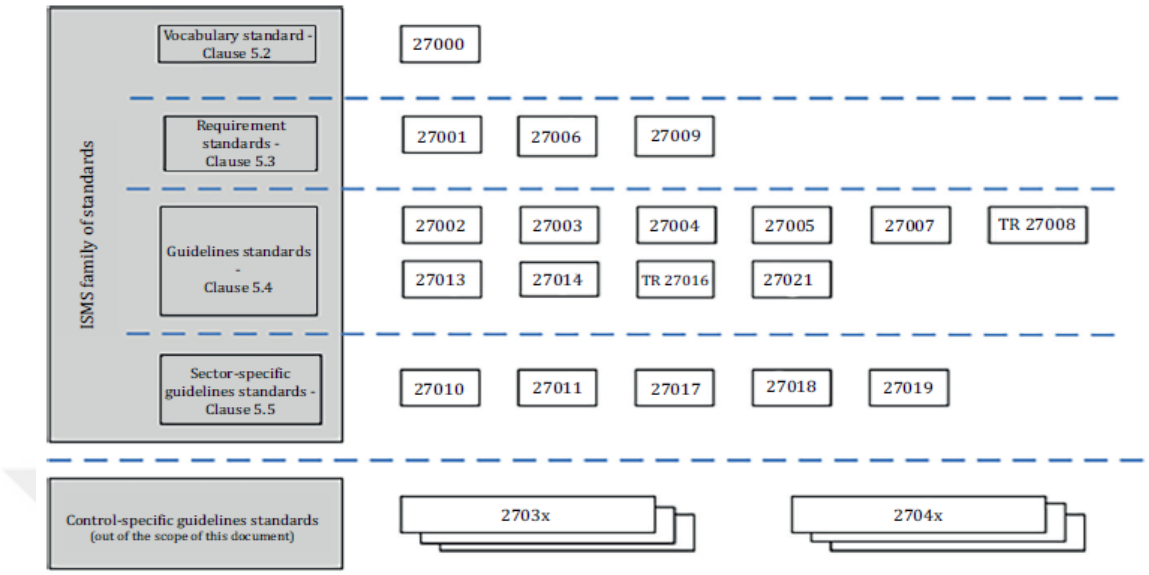

Figure 3. 1 The Components of This Standard Family Are Briefly

ISO / IEC 27001: the documentation of an Information security management system covers the planning, implementation, control and Prevention of all processes.

ISO / IEC 27002: used as a guide during the implementation of information security controls.

ISO / IEC 27003: provides guidance on the Information Security Management System requirements set out in ISO / IEC 27001 and offers recommendations, possibilities and permissions on them. Providing general guidance on all aspects of Information Security is not the purpose of this document (ISO/IEC 2017).

ISO / IEC 27004: designed to help them assess information security performance and the effectiveness of the Information Security Management System to meet monitoring, measurement, analysis and evaluation requirements (ISO/IEC 2020)

ISO / IEC 27005: this document supports the general concepts set out in ISO / IEC 27001 and is designed to assist in the satisfactory implementation of information security based on a risk management approach (ISO 2020).

ISO/IEC 27006: this international standard, ISO / IEC 17021-1 and ISO / IEC 27001 in addition to the requirements in the information security management system (ISMS) establishes

requirements and provides guidance for bodies providing auditing and certification of (ISO/IEC 2015).

ISO / IEC 27007: this document, in addition to the guidance in ISO 19011: 2011, provides guidance on the management of the Information Security Management System (ISMS) audit program, the conduct of audits and the adequacy of ISMS auditors (ISO/IEC 2017).

ISO / IEC 27011: the purpose of this standard is to define guidelines that support the implementation of information security controls in organizations operating in the field of telecommunications.

ISO / IEC 27799: the purpose of this standard is to define guidelines that support the implementation of information security controls in organizations operating in the health field.

ISO/IEC 27001: 2013 First, it developed in 1993 by the Ministry of trade and industry with the support of a group of leading international companies and organizations operating in the UK under the name Code of practice (CoP). The Information Security Management System (ISMS) standard subsequently published in 1995 under the name BS779. In Conjunction with the compilation of CoP applications by the British Standards Institute (BSI). There are two main objectives of the Code of practice (CoP):

Provide a common basis for organizations to effectively implement, develop and measure security management; and secure trade between companies.

These two main objectives are to minimize the impact of security events as possible and to ensure business continuity (von Solms, 1998).

The second part of the standard, BS7799-2, published in 1999. Later in 2000, after minor revisions under the name BS7799 - 1, it published by ISO under the name ISO/IEC–17799 and became an accepted standard worldwide.

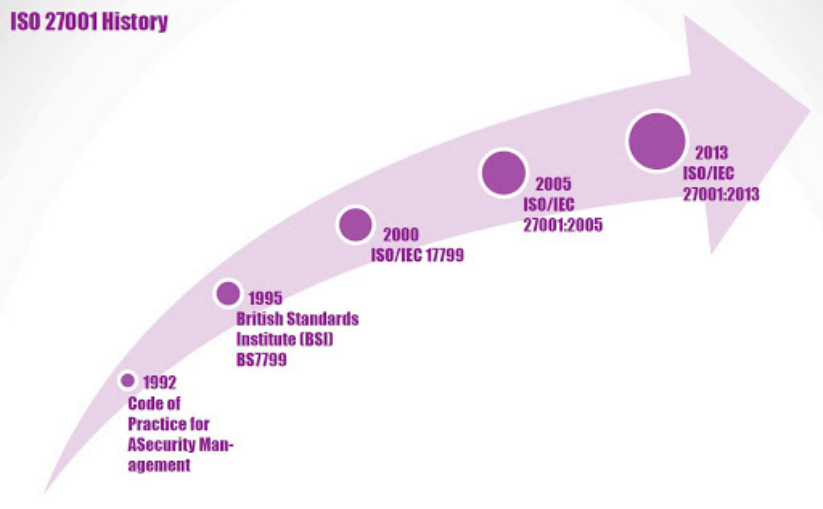

Figure 3. 2 ISO27001 History

BSI published it as a British standard in 2002 under the name BS–7799–2 with editing and additions on the first version. In 2005, ISO published ISO / IEC–17799 BSI as a British standard, with editing and additions on the first version in 2002 under the name BS–7799-2. In 2005, ISO ISO / IEC-17799 (Vural, 2007).

3.1.1. ISO 27001 concepts

This section includes the ISO27001 information security Management System standard, basic concepts that must understood or used in compliance processes.

Scope, the scope and limits to be applied must be determined first in the installation of ISMS. The scope of the ISMS may be the whole of the corporation, as well as only a part of it. For ISMS installation, it is very important that this scope fully and accurately defined. The scope is prepared by considering the intention of the administrators and the information security objectives of the corporation. There is no direct guidance of the standard itself in this regard. Since the scope may differ in corporation's terms, it expected that the corporation would be able to explain the reasons for which the issues excluded. Once the scope has been determined, it must document, published, and approved by the senior management. (UEKAE, 2008)

Context, the corporation needs to identify the internal and external issues affecting the achievement of the intended results of an Information Security Management System in accordance with its objectives. At the same time, the requirements of these matters should define

in terms of information security, including legal, regulatory requirements and contractual obligations.

Environmental factors that may or may affected by the corporation should taken into consideration when determining internal and external issues (Dilek, 2015).

Leader, installation and effective management of Information Security is the responsibility of senior management. Senior management is an integral part of isms and is directly responsible for ensuring that the corporation's information security strategies and objectives maintained and improved. It is responsible for ensuring compliance with information security requirements and corporation's processes. Ensure the supply of resources needed during the execution of isms. Continuous improvements need to support.

Information security policy, depending on the scope and context determined by the corporation, the information security policy of the corporation is determined. The designated ISMS policy, information security objectives of draw frame to put the business, legal or regulatory requirements, and contractual security obligations should consider. At the same time, the policy must include a commitment to meet and continuously improve applicable information security requirements. The information security policy must be available in writing, announced within the corporation, and accessible at any time by the relevant parties as appropriate.

Information security incident, an information security incident is a predefined occurrence that may result in a possible breakdown in the security policy of a service, system or network within the organization, or malfunction in protective elements or endanger security.

Risk, the most important issues in ensuring information security and establishing effective ISMS are the identification of information security risks and risk analysis. Risk within the framework of Information Security is the name given to events that may endanger all or any of the privacy, integrity and accessibility elements of information assets within the scope determined by the corporation. In other words, it can express as the uncertainties that may encountered during the operating process that intended to establish. For this reason, when identifying information security risks with the agency, it should consider the elements of privacy, integrity and

accessibility and calculate these risk assessment processes separately for these three elements (Çek, 2017).

While the 2005 version of the ISO27001 standard clearly stated that risks relate weaknesses and threats to assets, i.e. an asset-based risk analysis, the 2013 version of the standard removed this requirement and left the corporation more flexible in choosing methodology. The ISO 31000 standard cited as reference in the operation of Risk methodologies. When this reference examined, it seen that it contains recommendations for assigning risks to processes. The process of risk-based processing methods to organizations who want to track business processes, services processes and services are defined based on the relationship between beings with ISO 31000 give it to determine process-based risk analysis is to perform operations.

Applicability declaration, the declaration of applicability includes a description of which substances are included or excluded, the reasons for inclusion or exclusion and which are included in the checklist, known as Annex-A, contained in the standard. The Risk is the basis for decisions taken on handling (Çetinkaya, 2008).

Based on defined security requirements, it is necessary to establish security controls that ensure compliance with the organization's security requirements. The main documents used to establish safety checks are standard ISO/IEC 27002. This standard includes guidelines and recommendations on how to implement the safety controls included in the Annex-A list of ISO27001. The standard ISO27001 Annex A-list covering the requirements and objectives of the organization in the field of Information Security General controls and security controls consists of a set of 114 ISO / IEC 27002 standard separates into 14 main groups according to the area you operate the controls. Based on the identified security requirements of the organizations and the systems and technologies used by the organization, 114 security controls have been determined that must implemented in the organization. The whole process documented with the statement of applicability (Matúš, H. ve Martın J. 2009).

Internal audit, it is a collection of audits and practices carried out by corporations with an external independent auditor or in-house staff to determine whether the requirements of I set up have met, how active it is, whether it is being used effectively and whether it is missing or

wrong. It is also an important opportunity to determine the status of the corporation before the certification audit, which is the principal audit, carried out (Kemmler et al., 2018).

Control, in Turkey, certification audits can carry out by TSE and some accredited private corporations. The ability of a company to issue an ISO certificate depends on its accredited by the competent authorities for issuing certificates. TURKAK is the public authority to grant accreditation to all corporations in Turkey. According to TURKAK's data, the number of corporations accredited to issue ISO27001 certificates as of January 2019 is 36 (TÜRKAK, 2020) TURKAK is a member of the European Co-operation for Accreditation – ea, an international accreditation body, and considers the guidelines prepared by the international accreditation associations in its accreditation activities.

Independent auditors on behalf of independent audit firms carry out audits. The persons who will perform ISO27001 inspection expected to have certificates that are valid throughout the world. After the lead auditor training given by the competent training corporations, persons may have the right to conduct an audit of the information security management system in companies with the ISO27001 LA (Lead Auditor) certificate issued by the IRCA as a result of the examination (Kıraç, 2015).

The validity period of the certificate issued after the audit is 3 years. After the first certification inspection, supervision inspection carried out in 2nd and 3rd years in order to check the existence, continuity and effectiveness of the established ISMS.

3.1.2. ISO27001 Requirements and Processes

Steps and processes identified for the complete completion of ISO27001 standardization processes in this section. The effective execution of established ISMS is included.

Determining the scope and context, determining the context and scope of a corporation is one of the procedures required in ISO27001. Four of the standards. In this article, it stated that an organization must identify internal and external issues that may affect information security structuring and management planning.

At the stage of determining the context and scope, define the effects of various elements in the corporation and these elements include the information security management system, the goals, objectives and culture of the corporation, processes, the size of the corporation structure, stakeholders, etc. it means that the effects of drying should determined in terms of.

The Standard says that the context and scope of the corporation must be determined, but it does not provide information on exactly how it will be, except for some basic considerations. The main points mentioned can stated as follows:

Internal and external considerations, caution should exercise when determining internal and external considerations. Otherwise, the points determined may be either too comprehensive or too narrowly comprehensive to draw the overall picture. While working on this article, considerations that may affect information security should taken into consideration.

The internal context of a corporation is the environment in which it wants to establish ISMS. The internal context may include parties who have direct or indirect access to Information, produce and govern it. To determine the external context, social, economic, technological, environmental, legal, etc. problems from the environment can considered (Humphreys, 2018).

Related parties, in the installation of ISMS, the information security needs of these parties should well define by identifying the parties concerned with information security. These requirements of the parties concerned may include legal and contractual provisions. These parties may be directly affecting corporate information assets (ISO/IEC, 2013).

Documentation, it stated in the standard that all internal and external birches mentioned and the scope created accordingly should documented. They are the first documents requested by the certification bodies during the audit in order to have information about the corporation inspected and the department to be certified.

These documents should review at regular intervals and the necessary updates should made in a controlled manner with the approval of the relevant parties.

Determination of information assets, in order for an organization to operate its corporate processes, all of the information it has called information assets. In order for a corporation to

ensure information security, first, each corporation will be aware of its information assets. It will determine the importance and value of the assets it owns. In this process, corporate information assets need to be fully identified, their weaknesses identified and protected from unwanted threats and hazards. To protect these assets, physical security, communications security, the provision of integrated access security, as well as with different Secure Elements has to study in an organized manner (Baykara et al., 2013).

Determination of policies and procedures, an organization needs guidelines and instructions on how to plan and then implement the processes it creates to ensure information security, and how to improve the problems encountered during implementation.

Policies can be defined as formal instructions and statements produced and supported by senior management. They can be corporation -wide, subject-specific or system-specific. The corporation's policies should reflect its information security objectives.

The most fundamental of these policies is the Information Security Policy, which based on the specified coverage. This policy includes key topics such as the strategic approach of the organization, objectives, tasks and responsibilities, the will of senior management in leadership, and basic tasks and responsibilities during the ISMS operation process.

Within the scope of ISMS, a number of sub-policies should also draw up, with the Information Security Policy serving as the roof. Examples of these:

- Information Security Situation Monitoring Policy
- Information Security Incident Management Policy
- Information Systems Acquisition Development Policy
- Change Management Policy
- Audit and Compliance Policy
- Access Management Policy
- Physical and Environmental Safety Policy
- Secure Software Development Policy
- Human Resources security and in-service training policy
- Business Continuity Policy

- Cryptographic controls and Key Management Policy
- Stakeholder Information Security Policy
- Appropriate Use Policy
- Third Party Security Policy

Policies such as asset management policy can given.

Procedures are documents that contain systematic instructions to accomplish a specific purpose or task. Procedures related to Information Security, which frequently repeated in corporations, carried out through procedures. In this way, the operations to perform in a certain order, security controlled, minimum initiative and a quality manner ensured.

As an example of the procedures that can created within the scope of ISMS:

- Network and Network Devices management procedure
- Information Exchange Management Procedure
- Disciplinary Procedure
- Procedure for Managing External Services
- Document and record management procedure
- Corrective action and improvement procedure
- Activity measurement and evaluation procedure
- Safety tests and patch management procedure
- Internal Audit Procedure
- Business Continuity Procedure
- Capacity Management and system acceptance procedure
- Security Procedure against Malicious Software
- User Account and password management procedure
- Risk Assessment and processing procedure
- Server Management Procedure

- Remote Access Management Procedure
- Software Development Procedure
- Backup Procedure

Procedures such as management review procedure can given.

Identifying threats and weaknesses, incidents that may cause damage to the information assets of the corporation called threats. Threats can be internally sourced, such as corporate employees, or outsourced, such as malicious attackers, and human-based. On the other hand, technical internal threats such as failures in corporate systems or natural external threats such as floods, earthquakes, fires can consider as threats that can damage information assets. The threats that may occur during the installation and operation of ISMS should well identified and the damages that may occur should dealt with risk analysis.

On the other hand, if an information asset is likely to damage by a threat, it considered as a weakness of the relevant information asset. The possibility that the weaknesses that information assets have used by a threat is also considered a risk. For this reason, the inventory of the information assets of the corporation should taken out and the corporation's values of these assets should determine by determining their vulnerability in the face of threats. It should ensure that the corporation's threat and vulnerability register kept up to date by making these transactions periodically (Çek, 2017).

Risk assessment, information security risk assessment is the most important part of isms, which allows an organization to identify security vulnerabilities and threats and then decide what measures to choose to address potential threats (Shameli-Sendi et al., 2016)

Failure to conduct a risk assessment properly and regularly can have serious consequences for the corporation, such as loss of reputation, legal issues or even a direct financial impact.

The main objective of the Risk assessment process is to evaluate the source of the risk, its consequences if it occurs, its possibility, the types of scenarios that may encountered, the subsequent controls and the effectiveness of these controls, if the risks considered appropriate by examining them in terms of quality.

Different techniques can apply when performing Risk analysis. The techniques to use may vary according to the conditions and purpose of use. Risk analysis can do in the form of qualitative, quantitative or a mixture of these.

According to ISO 31000 standard, the factors to considered during risk analysis are as follows:

- Possible events and their probability
- Size of results
- Variability States
- Quality and size of results
- Effectiveness of controls
- Confidence levels

Because of Risk assessment, risks at the corporation's level can dealt with with a holistic approach. The risk assessment methodology should design to address the damages that information assets may face in terms of privacy, integrity and accessibility (ISO/IEC 2018)

Selecting controls, in order to achieve an effective, viable and continuously evolving I Management, appropriate control and objectives connected to these controls need to be determined. The ISO/IEC 27002 standard or other control sets can used when selecting controls. The special needs of the corporation should take into consideration when making the selection. For this reason, without adhering to any control set, the corporation-specific and corporation-designated controls can also create. For this reason, Control sets that are guiding must considered as starting points. On the other hand, when selecting controls, the risk acceptance criteria adopted by the corporation, risk processing options and the corporate risk management approach should take into consideration (Almeida, L. and Respício, A. 2018).

Handling risks, in Risk management, risks should treat as the second stage after assessing the risks. At this stage, it is necessary to decide how to handle the identified risks, to prioritize and to determine controls that will completely eliminate or reduce the risk. It is often impossible to eliminate the risks. For Risk processing, the risk processing processes shown in Figure 2.10 are applied. These processes can specify as:

Acceptance of risk, if there is no control to reduce or eliminate risk, IT systems continue to use with their existing condition.

Risk aversion, it is a measure taken in the form of a complete abandonment of the situation that causes risk. For example, stopping VPN access to remove external access risks.

Reducing risk, studies carried out in order to reduce the probability of the realization of the identified risks or to minimize the damages that may occur if they occur.

Transfer of risk, the transfer of the results to third parties without eliminating the risk. For example, insurance against possible damages. Corporate management is obliged to choose the most appropriate and least costly management in order to minimize losses to information assets during risk processing (Gaşpar, M.L. and Popescu, S.G. 2018).

Distribution of responsibilities and duties, in order to ensure that the ISMS meet the requirements of the ISO 27001 standard and to report to the senior management concerned with the performance of the established isms, it is necessary to identify, appoint and announce the responsibilities related to the Info-Sec management process by the management. Senior management may also appoint managers and staff to manage the ISMS process, although the ultimate responsibility is to protect the information assets of the organization.

Implementation of controls, the ISO 27001 standard seeks to ensure the provision of a living Information Security Management System. In other words, the established isms intended to gain a dynamic structure that can show instant reactions in the face of threats and attacks. For this reason, the ISO 27001 standard adopted the PDCA (plan-implement-control - act) cycle process model, shown in figure 2.3. In this model, checks can made on a regular basis whether all the processes applied implemented, whether necessary measures taken (Nurul, 2018).

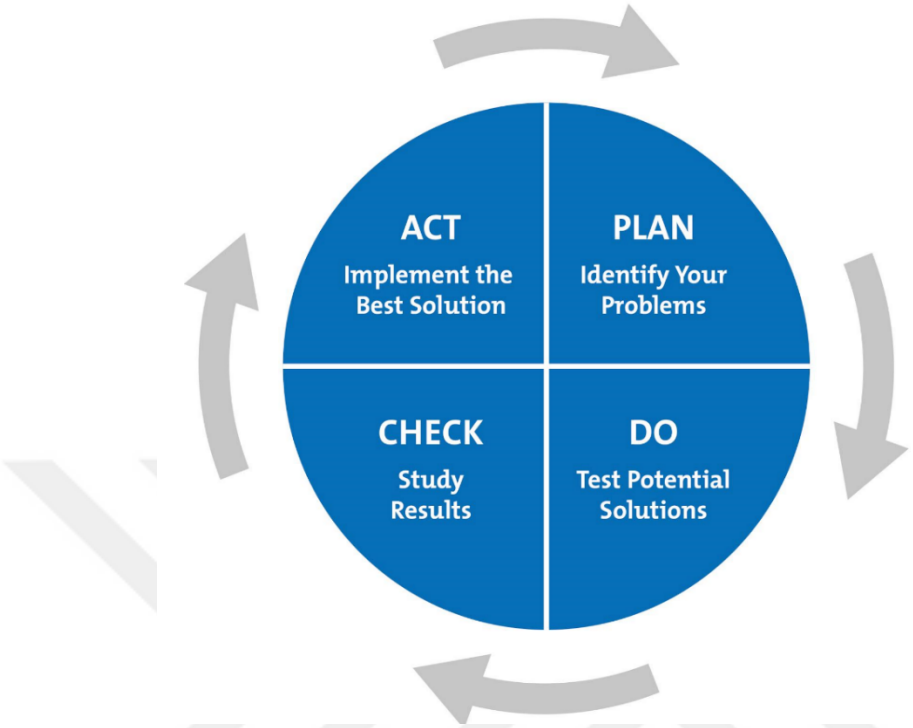

Figure 3. 3 PDCA Cycle

According to requirements and processes, planning has focused so far and the process from determining the scope to defining the risks has discussed. The implementation phase of the controls is the step in which all the activities, policies and procedures determined in the planning phase are implemented and the operation takes place. This step is very important because it will reflect the success of the ISMS (Nurbojatmiko 2016)

Monitoring performance, the corporation should evaluate the effectiveness of the isms it has established in order to determine the failures, deficiencies and innovations that may experienced during the implementation phase. At this stage, the corporation must decide for itself what should monitored and measured, including ISMS processes and controls that are expected to be implemented, and the measurement methods and tools that should be implemented to achieve the required monitoring results. Of course, in order to accept the selected methods and tools, it is necessary to produce output that is suitable for comparison and reproduction when requested.

3.2 ISO27001 Standards Worldwide

It is one of the most important internationally accepted standards, as the ISO 27001 standard defines the requirements of an Information Security Management System, is auditable and can be compatible with other management systems, regardless of the sector in which the relevant corporation operates. According to the statistics published by the ISO organization, it is stated that 31910 corporations, 2590 of which obtained in 2017, have ISO 27001 certificates. 15 countries with the highest ISO 27001 certificate are given in Table 3.1. In Turkey, according to the document number it seems to be 11th.

Table 3. 1 ISO27001 certificate numbers by country (2018) (ISO 2018)

	Country	**Certificates**
1	China	7,199
2	Japan	5,093
3	United Kingdom	2,444
4	India	2,161
5	Germany	1,057
6	Italy	1,041
7	United States of America	911
8	Taiwan, Province of China	827
9	Netherlands	788
10	Spain	726
11	Turkey	707
12	Poland	700
13	Romania	585
14	Czech Republic	543
15	Hungary	484

When the first 15 examined in the list created based on sectors, it seen that the corporations operating in the field of Information Technologies have the ISO 27001 certificate as of the end of 2018, as stated in Table 3.2, while the public corporations are in the 7th place.

Table 3. 2 Number of ISO27001 certificates by sectors in the world (2018) (ISO 2018)

	Sector	**Number**
1	Information technology	6,822
2	Other Services	893
3	Transport, storage and communication	369
4	Construction	309
5	Wholesale & retail trade, repairs of motor vehicles, motorcycles & personal & household goods	304
6	Engineering services	291
7	Public administration	281
8	Health and social work	278
9	Financial intermediation, real estate, renting	276
10	Electrical and optical equipment	227
11	Other social services	155
12	Education	137
13	Printing companies	130
14	Machinery and equipment	104
15	Electricity supply	64

4. RELATED RESEARCHES

In his master's thesis published by Çek (2017), he emphasized the importance of human factor in corporate information security governance. It emphasized that management support is essential for the management of information security governance in a healthy way and this support should given by top management. On the other hand, it stated that the support of the senior management is essential but not sufficient and all corporation staff should take an active role in this process. The importance of the awareness of the information security of the staff particularly emphasized, as it will negatively affect the information security processes of even a single staff member who is not involved in this process. In the process of raising awareness, it is very important to provide the necessary information and guidance within the framework of the corporate roles and responsibilities of each staff member.

In his PhD thesis published by King (2017), it aimed to investigate whether there is a linear relationship between corporate information security governance and Information security management standards. Within the scope of this study, a questionnaire applied on 210 people working in small and medium sized organizations in the USA, Hawaii and Alaska. Because of the survey, it has been determined that there is a linear relationship between effective information security governance and information security standards in organizations.

In his PhD thesis published by Güldüren (2015), it aimed to develop a website with multimedia materials and to raise awareness of this developed website in order to raise awareness of information security among faculty members working in higher education institutions. Within the scope of the study, the Information security awareness scale was developed. Because of the measurements made by the scale developed, it concluded that the website and other materials developed contributed positively to the awareness of information security.

Within the scope of the research conducted by Gencer (2015), it aimed to make the processes and requirements of ISO27001 dynamic and to become a part of daily life in corporations. In the related research, the requirement of ISO27001 standard expressed in order to gain corporations and international reputation and acceptance. It has stated that it has seen more in public corporations in recent years. In addition, it concluded that ISO27001 compliance studies should started by taking the inventory of corporate information assets. It concluded that in order to

manage the established system dynamically and to provide the necessary controls after the certification processes. It is necessary to get support from an application where the management of the system provided and at the same time, reducing the human factor, the weakest link of the system, as much as possible will affect the success positively.

Akay (2014), included the historical development of the ISO27001 standard and the differences between versions. In the related study, the interviews with two organizations that have completed the ISO27001 certification process and whose names hidden confidential are included and the findings discussed. Within the scope of the related study, it stated that ISMS processes perceived as a technical issue and this false perception negatively affects the effectiveness of established ISMS. On the other hand, it emphasized that parallelism should be provided in theory and practice during the implementation of ISO27001 requirements.

In the study conducted by Gürcan (2014), it focused on determining the information security needs of financial corporations under the umbrella of ISO27001. In this context, various questionnaires have applied to the relevant corporations. According to the results of the survey, it stated that the documentation section of the processes completed, but there were some problems in the implementation of organizational processes. It concluded that the policies developed especially on the mobile workforce side are not sufficient and they have a 75% competence in the implementation of other policies and procedures.

In his study on the implementation of ISO27001 and ISO27005 standards, Ganbat (2013) focused on how ISO27001 should applied and its relationship with the ISO27005 Risk Management standard. In the scope of the study, it emphasized that the relevant corporation or organization can determine the scope of ISO27001 and therefore, a detailed study should do during the determination of the scope, and support should obtain from the ISO27005 standard in order not to overcome any point. At the same time, it emphasized that management support is essential during the compliance process with standards.

In the study carried out by Demirtaş (2013), the success bases of ISMS conducted by public and private sector organizations evaluated and the factors that positively affect the system or examined. On the other hand, a model proposal made to ensure the effective implementation of ISO27001 certification processes. At the same time, it has evaluated that having ISO27001

certificate will positively affect the brand and image value of the related organizations. In the scope of the study, it emphasized that technical opportunities would not be sufficient to provide information security effectively, and that these opportunities should supported by staff awareness, processes, policies and procedures, and it concluded that this would be best possible through a certification process. It emphasized that information security is not only a technological process, but also the human factor should handle in detail, and necessary awareness studies and trainings should implement.

In his study titled "Information Security Standards and a Model Proposal for Public corporations Information Security", Haklı (2012) focused on developing an application designed specifically for public corporations and managing all ISO27001 installation processes. Within the scope of the study, it emphasized that the first addressee is the IT Centers of the corporations where the information assets are processed, stored and managed in order to start the ISMS installation studies. These software studies worked with information processing centers during the analysis stages and a private information security model created for public corporations.

In a thesis study carried out by Shoraka (2011), he researched whether the possession of a certificate brings any economic value to the relevant organizations with a research he has conducted among the organizations that have completed the ISO ISMS certification process. Because of the said research, a determination has made that there is no increase in value, especially after the announcement of the certification of the corporations in the capital markets. It concluded that the ISO ISMS certification process does not bring any economic value to the relevant organizations, since there is no difference between the responses to information security violations between the certification bodies and non-organizations.

In the study conducted by Mete (2010), the application of ISO27001 standard to data processing centers investigated. Within the scope of the study, it aimed to create a Turkish resource that serves as a guide to the data processing centers that want to install ISMS. In addition, the importance of management support during the establishment and management of ISMS, as well as the importance of the presence of a team with a high level of knowledge about the standard, which dominates the corporate processes. At the same time, it stated that the relevant processes should not only be with the ISMS team, but should spread across the floor, and the necessary

will to shown to ensure the necessary contributions of all relevant units. It emphasized that ISMS is especially a risk management process and the importance of identifying corporate information security risks and managing risk processes effectively, and all details should examine within this process. For this reason, the importance of ownership of the ISMS to establish by the whole corporation has emphasized.

In the study prepared by that Aydogdu (2010) "Information Security of the Organization in Turkey Maturity Determining the Level and ISO / IEC 27001: 2005 Assessment of Standards Compliance" information security of the corporations as part of the thesis was to determine the maturity level. Within the scope of the data obtained from the survey questions prepared within the scope of the study, the following results obtained. It observed that the information services, finance, insurance, telecommunications, health and real estate sectors have completed their information safe control and duties largely. It is also aware of the necessity of the management standard in many organizations.

5. RESEARCH AND METHODS

In this section, the studies on how to do the research, the universe and the sampling and data collection emphasized.

5.1. Research Model

A descriptive study carried out in order to determine the subjects such as the extent to which the public broadcasting corporations that possess and certify an Information Security Management System possess this process, whether having a certificate is sufficient in ensuring information security, and the improvement in Information security awareness levels. Survey studies carried out on the samples of this study and the main problems and sub-problems tried to be answer in line with the answers received. The data obtained are in the SPSS (Statistics Package for Socials Sciences) package program. Male and female employees' values for all categories are explained for public broadcasting corporations in four continents all around the world as follows. 77 female and 79 male employees for Management, 38 female and 50 male employees for Information Security Staff, 70 female and 110 male employees for Tech Staff, 381 female and 701 male employees for Other Staff. Percentage, independent groups t-test was used in the solution of this data. According to the t-test results, the general average value of managers was determined as 3.92, df 154. According to the t-test results, the general average value of Information Security Staff was determined as 3.25, df 86. According to the t-test results, the general average value of Tech Staff was determined as 3.80, df 178. According to the t-test results, the general average value of Other Staff was determined as 3.49, df 656.

5.2.Universe and Sampling

The universe of the research consists of public broadcasting corporations that have ISO27001 certification worldwide. Because the universe is large and some ISO27001-owned corporations and organizations not allowed applying questionnaires to corporation's staff, the participation of the authorized corporations has not fully achieved. The sample of the research consists of public broadcasting corporations with their ranking of ICT Development Index in 2017 below. Those are in Europe, (Turkey #67, Germany #12, United Kingdom #5) America, (USA #16, Canada

#29, Mexico #87) Asia, (Qatar #39, Japan #10, Korea Rep. 2#) Ocenia, (Australia #14, New Zealand #13) and 1082 people working in these corporations.

5.3. Data Collection Tools

The study consists of four questionnaires prepare to be applied to four different staff groups (Management, Information Security Staff, Tech Staff and Other Staff) currently working in public broadcasting corporations that hold ISO27001 certificates worldwide in four continents. The questionnaires shared with all people via online survey. All prepared questionnaires consist of two main sections. In the first section, demographic information of the people such as age, gender, education and occupation requested, while in other sections questions related to their target audience were included. In the questions in the second sections, Cronbach's Alpha (α) reliability analysis applied to the 5-point Likert scale. After the reliability analysis and reverse analysis results, it concluded that the reliability levels of the questions prepared sufficient. The ratings of the scale are "Strongly disagree", "Disagree", "Indecisive", and “Agree", "Strongly agree". The questionnaire questions created by taking the opinions of the experts in the fields of information security and statistics. While preparing the questions, care has taken to ensure that they are understandable and do not cause different understandings among the participants.

"It is not acceptable to exclude any of the conditions specified in Articles 4 to 10 if an organization claims to comply with this standard, which is included in the ISO27001 standard during the creation of the survey questions." The related articles mentioned in the statement and various thesis studies prepared before about information security used. The data regarding the surveys created and analyzes applied are as follows:

5.4. Management

The questionnaire prepared for the managers of the corporation consists of 16 questions. With the questionnaire questions, it aimed to examine one of the indispensable elements of ISO27001 and at the same time under the fifth Leadership clause of the relevant standard, their approach to the role of "Leadership" and their will to operate and operate the system.

In this context, questions 1, 2, 10, 11 and 12 of the questionnaires prepared for managers indicate that the management level should show leadership and loyalty in relation to the Information

Security Management System, and that continuous improvement should support. It prepared based on the statements and aimed to get the opinions of the related parties on this issue. The third and fourth questions of the executive questionnaire have been prepared based on the statement that it is necessary to reach the corporate strategic targets and to comply with the corporate processes in 5.1.a and 5.1.b of ISO27001 standard. On the other hand, the fifth question of the said questionnaire has been prepared in order to get the opinions on the matter regarding the studies on providing information security awareness in article 7.3 of the related standard. The 6th, 7th and 8th questions of the questionnaire prepared in order to get the opinions of the relevant parties regarding the corporation's ISMS policy included in the articles 5.2 and 5.3 of the ISO27001 standard and the roles and responsibilities in the established ISMS. The ninth Question included in the questionnaire is to obtain the opinions of the Management regarding the measures under the title of "A.9.2.3 Management of privileged access rights", which is one of the control items of Annex-A of the standard. Because of the analysis of the preliminary study, the reliability coefficient of the management survey calculated as 0.921.

5.5. Information Security Staff

Problems experienced during the work of the information security staff, who are problematic about the operation of ISO27001 in the corporations and providing the necessary controls, and appointed by the senior management, tried to be address and their competency levels tried to question. The questionnaire prepared for Information security staff consists of 18 questions. After the expert opinions, two questions removed. The reliability coefficient of the management questionnaire calculated as 0.867 after the analysis of the preliminary study.

In this context, while preparing the survey questions in order to applied to the Information security members, the requirements and responsibilities regarding the Information security staff included in the ISO27001 standard taken into consideration. The questions between the 1st and 5th questions are aimed to get the opinions of the Information security staff about the necessity of providing the necessary trainings and ensuring the competencies in order to ensure the effective execution of the Information security management processes under the 7. Support title of the relevant standard. While creating the sixth, seventh and eighth questions, it is aimed to get opinions on the compliance and effectiveness of the work with the corporation's staff during the

realization of the activities that address the 6.1 risks and opportunities of the relevant standard. On the other hand, among the 9th and 14th questions, it aimed to get the opinions regarding the commitment to the Information Security of the board and the ownership of the processes, which are also under the article 5.1 of the ISO27001 standard.

5.6.Tech Staff

In the question set prepared for the technical teams of the corporations, it aimed to question the will and competencies that the team has shown to fulfill the requirements of ISO27001. The questionnaire prepared for the tech staff consists of 17 questions. After the expert opinions, one question removed. After the analysis of the preliminary study, the reliability coefficient of the management questionnaire calculated as 0.932.

In this context, the duties and responsibilities applied by the ISO27001 standard for the mentioned teams taken into consideration in the questions created to apply to the technical teams of the corporation and it aimed to get their opinions on these duties and responsibilities. In particular, there are instructions for determining the required competencies for the technical staff affecting the performance of information security in article 7.2.a of the Standard and that these qualifications. It should provide in article 7.2.b. Questions 1 and 3 of the relevant questionnaires prepared within this scope and it aimed to get the opinions of the tech staff on these issues. On the other hand, there are instructions that the performance of ISMS, which managed under the main headings 9 and 10 of the ISO27001 standard, should monitored at certain intervals and the determined deficiencies should eliminated through the studies. It aimed to take the opinions of the technical team about the contributions of the relevant standard in the point of monitoring, evaluation and continuous improvement of all questions between the 4th and 11th questions of the questionnaire in question.

5.7.Other Staff

In the question set prepared for the other staff based on non-tech departments, the approach of the other staff and the satisfaction levels of the process regarding the awareness raising process that is required to realize regarding the awareness of the staff side required by ISO27001 tried questioned. The questionnaire prepared for the other staff consists of 16 questions. After the

expert opinions, three questions removed. The reliability coefficient of the management questionnaire calculated as 0.854 after the analysis of the preliminary study.

Due to the human element, the effectiveness and continuity of corporate information security management constantly questioned. For this reason, the human factor, which is one of the three basic elements of information security, is one of the factors that ISO27001 standard emphasizes. The fact that processes are associated with people in many parts of the standard is one of the most important indicators of this. In the survey questions prepared for the end users, which are the weakest link in the information security processes, it planned to get the opinions of the staff on the topics under the seventh Support main topic, which especially focuses on awareness issues. Particularly, according to the instructions under the title A.7.2.2 from the ANNEX-A controls, the questionnaire questions and the opinions of the staff tried to obtain regarding the awareness trainings that should organized at certain intervals.

5.8. Collection of Data

The surveys prepared to be applied both to the website prepared specifically for the survey and public broadcasters to the outputs.1150 questionnaires answered, and 68 of these answered questionnaires were not taken into consideration due to missing answers. The 1082 questionnaires evaluated; 156 of them by management and unit managers, 88 of them by Information Security staff, 180 of them by Tech Staff and 658 of them by other staff answered of them. The questionnaires distributed as 381 female and 701 male employees. The distribution of the surveys by public broadcasting corporations per continents given in Table 5.1. The names of the corporations kept confidential for security reasons and according to the permissions received from the corporations (Africa’s answers not added due to insufficient information).

Table 5. 1 Distribution of surveys by public broadcasting corporations per continents

Corporations in	**AMERICAS**	**ASIA**	**OCENIA**	**EUROPE**	**Total**
Management	42	40	26	48	**156**
Info. Sec. Staff	22	26	12	28	**88**
Tech Staff	44	40	44	52	**180**
Other Staff	112	138	110	298	**658**
Total	**220**	**244**	**192**	**426**	**1082**

5.9.Solution and Interpretation of Data

The data obtained about the research analyzed in the appropriate survey and then explained, interpreted by creating tables. The staffs have completed the ISO / IEC certification process and are in the management level in public broadcasting corporations with active ISMS Information security staff who are responsible for the establishment and effective management of the corporate ISMS. That assigned by the management, ISO27001 percentage distributions used to determine the opinions of non-technical staff in the public broadcasting corporations, other than the Information security staff, who is indirectly responsible for information security, and the Tech Staff, where Information security standards are effectively implemented, other than the Information Security staff of the public broadcasting corporations.

6. RESEARCH FINDINGS

In this section, the findings about the survey data applied within the scope of the thesis research and the comments made in line with these findings are given. Each questionnaire examined under a separate subtitle.

6.1. Opinions of Management on Information Security Management System

In this section, the data obtained by the top managers or unit managers working in public broadcasting corporations that have ISO27001 and who are participating in the research would be examine. It seen that 156 management executives of public broadcasting corporations in four continents participated in the survey. The questionnaires distributed as 77 female and 79 male employees. The survey consists of 12 questions. The data regarding the answers given by the managers to the questionnaires analyzed on a question basis.

6.2. Opinions about the necessity of ISO 27001 Standard for corporations

The percentage distribution of the answers given to the questions about whether the management level is necessary for the corporations of ISO27001 standard given in Table 6.1.

Table 6. 1 Question 1- answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	3,8	3,8
Disagree	8	5,1	9,0
Indecisive	2	1,3	10,3
Agree	46	29,5	39,7
Strongly Agree	94	60,3	100,0

When the given responses examined, 94 of 156 executives (77 female, 79 male) who participated in the survey gave the answer "Strongly agree" and 46 of them answered "Agree". In this context, it seen that 140 people agree with the idea that ISO27001 is required for their corporations. The standard deviation values of female managers determined as .923 and the

mean value is 4.42. The standard deviation values of male managers are 1.165 and the mean value was 4.28. df 154 and significant value are .260 on independent samples based on t-test result. From this point of view, it can conclude that the idea of managers in general is essential for the corporations of ISO27001.

6.3.Opinions about national and international reputation of ISO27001 certification

Percentage distributions regarding the responses given by the managers about whether ISO27001 certification has national or international reputation given in Table 6.2.

Table 6. 2 Question 2 - answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	4	2,6	2,6
Disagree	8	5,1	7,7
Indecisive	16	10,3	17,9
Agree	54	34,6	52,6
Strongly Agree	74	47,4	100,0

When the given responses examined, it can see that 47.4% of the respondents expressed positive opinion as "Strongly agree" and 34.6% "Agree". The standard deviation values of female managers determined as .947 and the mean value is 4.30. The standard deviation values of male managers are 1.028 and the mean value was 4.09. df 154 and significant value are .794 on independent samples based on t-test result. It observed that the positive opinion dominates the point that the ISO27001 certificate gives the corporations dignity.

6.4. Opinions about the convenience it provides to my corporate goals in Information Security

Percentage distributions of the answers given to the question asked about the convenience and contributions of having the ISO27001 certificate in reaching the targets to the relevant corporations given in Table 6.3.

Table 6. 3 Question 3 - answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	12	7,7	7,7
Disagree	2	1,3	9,0
Indecisive	8	5,1	14,1
Agree	64	41,0	55,1
Strongly Agree	70	44,9	100,0

When the answers given analyzed, the general opinion is positive. It seen that the participants answered the question as “Strongly agree” and 41% as “Agree by 44.9%. The standard deviation values of female managers determined as 1.062 and the mean value is 4.29. The standard deviation values of male managers are 1.144 and the mean value was 4.00. df 154 and significant value are .589 on independent samples based on t-test result.

6.5. Opinions of ISO27001 Information Security policies on the benefits of corporate processes

Percentage distributions of the answers given to the question posed by the managers that having ISO27001 certificate does not make any positive contribution in the implementation of corporate business processes given in Table 6.4.

Table 6. 4 Question 4 - answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	2	1,3	1,3
Disagree	14	9,0	10,3
Indecisive	6	3,8	14,1
Agree	62	39,7	53,8
Strongly Agree	72	46,2	100,0

When the given responses examined, based on this result it seen that the general opinion is positive. The standard deviation values of female managers determined as .963 and the mean value is 4.31. The standard deviation values of male managers are .969 and the mean value was 4.10. df 154 and significant value are .508 on independent samples based on t-test result. 46.2% of respondents "Strongly agree", while 39.7% "Agree" reported in the form of opinions.

6.6.Opinions of ISO27001 corporate administrators about their contribution to Information Security awareness

Percentage distributions of the responses given by the corporation managers to the related question regarding “creating information security awareness”, which is one of the most important duties of ISO27001, given in Table 6.5.

Table 6. 5 Question 5 - answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	2	1,3	1,3
Disagree	12	7,7	9,0
Indecisive	6	3,8	12,8
Agree	50	32,1	44,9
Strongly Agree	86	55,1	100,0

When the given responses examined, 55.1% of the executives expressed their opinion as “Strongly agree” and 32.1% stated that “Agree”. The standard deviation values of female managers determined as .921 and the mean value is 4.40 The standard deviation values of male managers are .990 and the mean value was 4.24. df 154 and significant value are .831 on independent samples based on t-test result. It can see from here that ISO27001 provides a positive opinion that it provides benefit in creating awareness of information security. On the other hand, it seen that one person stated, “Strongly disagree”, six people stated “Disagree” and three people were indecisive about this issue.

6.7. Opinions about the contribution of management support to the sustainability of the Information Security Management System

Percentage distributions of the responses given by the participants in the point of showing the necessary will behind the established system and management support, which is an indispensable part of ISO27001, given in Table 6.6.

Table 6. 6 Question 6 - answer distribution of Management survey

	Number. of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	3,8	3,8
Disagree	6	3,8	7,7
Indecisive	8	5,1	12,8
Agree	22	14,1	26,9
Strongly Agree	114	73,1	100,0

When the given responses examined, it seen that 73.1% of the managers stated “Strongly Agree”, 14.1% said “Agree” and the positive response is dominant in this regard. The standard deviation values of female managers determined as .927 and the mean value is 4.49. The standard deviation values of male managers are 1.119 and the mean value was 4.48. df 154 and significant value are .487 on independent samples based on t-test result.

6.8. Opinions of the management regarding the applicability of the duties included in the ISO27001 Information Security Management System

Percentage distributions of the answers given to the question asked whether the duties and responsibilities of the ISMS, which established after the establishment of ISMS standardization, have imposed on the management of the corporation given in Table 6.7. The standard deviation values of female managers determined as .932 and the mean value is 4.12. The standard deviation values of male managers are 1.118 and the mean value was 3.86. df 154 and sig are .712 on independent samples based on t-test result.

Table 6. 7 Question 7 - answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	8	5,1	5,1
Disagree	6	3,8	9,0
Indecisive	18	11,5	20,5
Agree	72	46,2	66,7
Strongly Agree	52	33,3	100,0

It observed that 33.3% of the executives expressed their opinion as “Strongly agree” and 46.2% as “Agree” and gave a positive answer in this regard. It observed that nine people who correspond to a section of 11.5% are indecisive in this regard. The standard deviation values of female managers determined as 1.062 and the mean value is 4.29. The standard deviation values of male managers are 1.144 and the mean value was 4.00. df 154 and significant value are .032 on independent samples based on t-test result.

6.9.Opinions of the implementation of ISO27001 standards on the additional workload brought by the implementation of corporate processes

The participants asked their opinions on whether the ISO27001 standard imposed any workload during the implementation of corporate processes. Percentage distributions of the answers given to the relevant question given in Table 6.8.

Table 6. 8 Question 8 - answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	28	17,9	17,9
Disagree	24	15,4	33,3
Indecisive	44	28,2	61,5
Agree	40	25,6	87,2
Strongly Agree	20	12,8	100,0

When the given responses examined, it seen that the distributions on the positive and negative sides are close to each other and the highest response rate given with 28.2% is “indecisive”. In addition, 17.9% of the participants say, “Strongly disagree”, 15.4% responded as "Disagree" and stated that it does not impose a workload. On the other hand, 12.8% responded as "Strongly Agree", 25.8% responded as "Agree" and ISO27001 processes added to them. It observed that they responded that it brought the burden. The standard deviation values of female managers determined as 1.345 and the mean value is 3.08. The standard deviation values of male managers are 1.228 and the mean value was 2.92. df 152 and significant value are .032 on independent samples based on t-test result.

6.10. Opinions of ISO27001 Information Security and Management System as management about its privileges within this system.

Percentage distributions regarding the answers given to the question about whether the staff who are in the status of manager within the scope of ISMS established should privileged or not are given in Table 6.9.

Table 6. 9 Question 9 - answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	26	16,7	16,7
Disagree	32	20,5	37,2
Indecisive	30	19,2	56,4
Agree	40	25,6	82,1
Strongly Agree	28	17,9	100,0

Since the question asked contains a negative expression, reverse coding made during the evaluation of the answers given. When the given responses examined, the managers It can seen that 17.9% of them responded as “Strongly agree” and 25.6% of them agree that they should privileged by answering “Agree”. On the other hand, 16.7% responded as “Strongly Disagree”, 20.5% responded as “Disagree” and stated that they should not privileged and the remaining 19.2% are indecisive about this issue. The standard deviation values of female managers determined as 1.427 and the mean value is 3.21. The standard deviation values of male managers are 1.290 and the mean value was 2.95. df 152 and significant value are 0.21 on independent samples based on t-test result.

6.11. Opinions of external and internal security provided by ISO27001

Percentage distribution information regarding the answers to the question asked about the thoughts about whether the corporations holding ISO27001 have protection against the dangers that may come from outside the corporation as well as the dangers that may come from within the corporation given in Table 6.10. When the given responses examined, it evaluated that the general opinion is positive.

Table 6. 10 Question 10- answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	2	1,3	1,3
Disagree	12	7,7	9,0
Indecisive	18	11,5	20,5
Agree	94	60,3	80,8
Strongly Agree	30	19,2	100,0

It seen that 19.2% of the respondents responded as "Strongly Agree", 60.3% responded as "Agree", 11.5% reported indecisive opinion, and the rest reported negative opinion. The standard deviation values of female managers determined as .850 and the mean value is 3.96. The standard deviation values of male managers are .848 and the mean value was 3.81. df 154 and significant value are .796 on independent samples based on t-test result.

6.12. Opinions about the protection that ISO27001 will provide against general and local security problems

Percentage distribution information regarding the answers to the question asked about the opinions of the ISMS owned by ISO27001 regarding the possible information security events and whether they can protect the corporation and the staff of the corporations are given in Table 6.11. When the given responses examined, it evaluated that the general opinion is positive.

Table 6. 11 Question 11 - answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	2	1,3	1,3
Disagree	16	10,3	11,5
Indecisive	18	11,5	23,1
Agree	98	62,8	85,9
Strongly Agree	22	14,1	100,0

It seen that 11.5% responds as "Strongly Disagree" and "Disagree". On the other hand, it seen that 14.1% of the respondents responded as "Strongly Agree" and 62.8% responded as "Agree". The standard deviation values of female managers determined as .894 and the mean value is 3.79. The standard deviation values of male managers are .831 and the mean value was 3.77. df 154 and significant value are .496 on independent samples based on t-test result. From this point of view, it seen that the contribution of the majority will be positive for ISO27001.

6.13. Opinions about the relationship between ISO27001 certification and the efficiency of the established ISMS

Percentage distribution information regarding the answers given to the question asked whether ISO27001 certification is required for, managing the ISMS owned by corporations efficiently and effectively given in Table 6.12.

Table 6. 12 Question 12 - answer distribution of Management survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	8	5,1	5,1
Disagree	24	15,4	20,5
Indecisive	28	17,9	38,5
Agree	64	41,0	79,5
Strongly Agree	32	20,5	100,0

When the responses given analyzed, 20.5% of the participants responded as “Strongly Agree”, 41% of them responded as “Agree”, and the certification is required at the point of effectiveness, 20.5% of them are “Strongly Disagree” and “Disagree”. The standard deviation values of female managers determined as 1.109 and the mean value is 3.65. The standard deviation values of male managers are 1.153 and the mean value was 3.48. df 154 and significant value are 1.000 on independent samples based on t-test result. It seen that no certification is required for ISMS management, and approximately 17.9% of them say, “I am indecisive”.

6.14. Information Security Team Opinions about Information Security Management System

In this section, the data obtained from the staff responsible for the establishment and operation of Information Security, which have ISO27001 public broadcasting corporations, will be examine. 88 staffs from public broadcasting corporations participated in four continents all around the world in the survey. The questionnaires distributed as 38 female and 50 male employees. In the questions asked, it planned to take the opinions of the Information Security staff about their duties and their opinions about ISMS. The answers given by the participants to the survey questions examined on a question-based basis.

6.15. Opinions about the necessity of consultancy services to manage Information Security Management System processes

It is possible that a large part of the corporation's purchases consultancy services from professional organizations since their staff do not have sufficient experience in the establishment and management of ISMS. Percentage distribution information regarding the answers given to the staff who are in charge of carrying out ISMS services and ensuring their continuity, whether there is a need for consultancy service in their corporations are given in Table 6.13.

Table 6. 13 Question 1- answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	6,8	6,8
Disagree	10	11,4	18,2
Indecisive	12	13,6	31,8
Agree	30	34,1	65,9
Strongly Agree	30	34,1	100,0

When the given responses examined, it seen that the answers of the participants "Definitely Agree" and "Agree" were equal to 34.1%. From this, it can conclude that most of the consultancy services are required. On the other hand, it seen that 6.8% of the answer is "Strongly Disagree", 11.4% of the "Disagree" answer, and consultancy service is not needed, and 13.6 part of them gave indecisive opinions. The standard deviation values of female information security staff determined as 1.228 and the mean value is 3.71. The standard deviation values of male information security staff are 1.240 and the mean value was 3.82. df 86 and significant value are .848 on independent samples based on t-test result.

6.16. Opinions of corporation staff about the adequacy of the Information Security Management System processes

It is compulsory that the members of the Information Security team, formed for the purpose of managing the ISMS processes, ensuring their continuity and continuous improvement, are

composed of the corporation staff and the necessary assignments are made by the senior management. In this context, percentage distribution information regarding the answers given to the question about whether information security staffs are sufficient for the management and continuity of the related processes given in Table 6.14.

Table 6. 14 Question 2 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	8	9,1	9,1
Disagree	16	18,2	27,3
Indecisive	38	43,2	70,5
Agree	22	25,0	95,5
Strongly Agree	4	4,5	100,0

When the responses given analyzed, it seen that the participants mostly consider the staff of the corporation insufficient or are indecisive on this matter. It observed that only 29.5% of the respondents gave a positive opinion on this issue, with 4.5% of the respondents saying, "Strongly agree" and 25% of the respondents said “Agree ". On the other hand, it observed that the majority of the participants were indecisive about the qualifications with the answer of “I am indecisive” of 43.2%. These values support the view that the overall evaluation is negative. The standard deviation values of female information security staff determined as 1.040 and the mean value is 3.00. The standard deviation values of male information security staff are .968 and the mean value was 2.96. df 86 and significant value are .800 on independent samples based on t-test result.

6.17. Opinions Information Security Staff ' about their training needs

Percentage distribution information regarding the answers given to the question about whether Information Security staff need any training in order to operate information security processes, related policies and procedures effectively and defined risks are given in Table 6.15.

Table 6. 15 Question 3 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	6,8	6,8
Disagree	4	4,5	11,4
Indecisive	4	4,5	15,9
Agree	18	20,5	36,4
Strongly Agree	56	63,6	100,0

When the responses given analyzed, 63.6% of the respondents responded as "Strongly Agree" and 20.5% of them agree that "Agree" and that the Staffs have training needs and the remaining 16% do not have any abstaining or needing in this regard. They appear to express their opinions. The standard deviation values of female information security staff determined as 1.141 and the mean value is 4.32. The standard deviation values of male information security staff are 1.230 and the mean value was 4.28. df 86 and significant value are .463 on independent samples based on t-test result.

6.18. Opinions of Staff about whether they should consist of Tech staff

Percentage distribution information regarding the answers given by the Staff to the question whether the Staff should form by the top management to manage the corporate ISMS processes should given in Table 6.16.

Table 6. 16 Question 4 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	6,8	6,8
Disagree	22	25,0	31,8
Indecisive	22	25,0	56,8
Agree	26	29,5	86,4
Strongly Agree	12	13,6	100,0

When the given responses examined, it seen that there is no consensus among the participants and the opinions did not focus on any answer. Regarding the question in question

32% responded as "Strongly disagree" and “Agree ", suggesting that some of them should not be comprised of IT staff members of the Information Security team, 25% of them abstaining and the remaining 43% said "Strongly agree" and "Agree" by answering, it seen that Information Security Staff expressed their opinion that they should consist of information staff. The standard deviation values of female information security staff determined as 1.166 and the mean value is 3.13. The standard deviation values of male information security staff are 1.166 and the mean value was 3.22. df 86 and significant value are .715 on independent samples based on t-test result.

6.19. Opinions about the number of Information Security Staff

Percentage distribution information regarding the answers given by the Staff to the question about whether the number of Staff created by the top management to manage the corporate ISMS processes is sufficient to manage the processes in a healthy way given in Table 6.17.

Table 6. 17 Question 5 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	10	11,4	11,4
Disagree	24	27,3	38,6
Indecisive	24	27,3	65,9
Agree	24	27,3	93,2
Strongly Agree	6	6,8	100,0

When the given responses examined, the standard deviation values of female information security staff determined as 1.085 and the mean value is 2.89. The standard deviation values of male information security staff are 1.175 and the mean value was 2.92. df 86 and significant value are .404 on independent samples based on t-test result. It seen that there is no consensus among the participants; the general opinion could be evaluated negatively. Regarding the question in question, “Strongly Disagree”, “Disagree” and “Indecisive” by expressing the opinion. That 66% of the group is that the members of the information security staff are numerically insufficient or the remaining 34% of those who are abstaining from this issue and “Agree” and It seen that by responding in the direction of “Strongly Agree”, the number of information security staff is sufficient.

6.20. Opinions about work compatibility between Information Security team and corporation staff

Percentage distribution information regarding the answers given by the Staff given in Table 6.18 to the question whether the Information Security Staff are working in harmony with the staff of the corporation, which is one of the most important stakeholders of the system, in order to manage the ISMS processes effectively and healthily.

Table 6. 18 Question 6 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	4	4,5	4,5
Disagree	16	18,2	22,7
Indecisive	30	34,1	56,8
Agree	30	34,1	90,9
Strongly Agree	8	9,1	100,0

When the given responses examined, 4.5% of the respondents stated that they “Strongly disagree”, 18.2% stated. They disagree “disagree”, 34.1% of them were indecisive on this issue and the remaining 43.2% and “Strongly agree” and “Agree”, and it seen that they gave a positive opinion that they can carry out a healthy work with the staff of the corporation. The standard deviation values of female information security staff determined as 1.085 and the mean value is 3.11. The standard deviation values of male information security staff are .942 and the mean value was 3.36. df 86 and significant value are .538 on independent samples based on t-test result.

6.21. Opinions about conducting corporate risk studies

It is necessary to identify the corporate risks, which is one of the most important elements of the works carried out within the scope of ISMS, and to follow the studies to carry out on the identified risks and to minimize the possible effects of the risks. In order to operate these studies in a healthy and effective manner, the studies conducted with the staff of the corporations are of great importance. In this context, percentage distribution information regarding the answers given by the Staff to the question about whether the support expected by the corporate staff can obtained during the operation of the corporate risk processes is given in Table 6.19.

Table 6. 19 Question 7 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	8	9,1	9,1
Disagree	30	34,1	43,2
Indecisive	20	22,7	65,9
Agree	28	31,8	97,7
Strongly Agree	2	2,3	100,0

When the given responses examined, it evaluated that the general opinion is negative. The corporation stated that 43.2% of the participants expressed negative opinions as "Strongly Disagree" and "Disagree", 23% remained indecisive about this issue, and the remaining 34% expressed their opinion as "Strongly Agree" and "Agree". It seen that they give a positive opinion about the fact that they can get enough support in the operation of risk processes with their staff. The standard deviation values of female information security staff determined as 1.069 and the mean value is 2.79. The standard deviation values of male information security staff are 1.043 and the mean value was 2.88. df 86 and significant value are .987 on independent samples based on t-test result.

6.22. Opinions on the applicability of ISO27001 processes

Percentage distribution information regarding the answers given by Staff to the question about whether the studies carried out within the scope of ISMS and corporation’s ISMS processes can applied in a healthy way given in Table 6.20.

Table 6. 20 Question 8 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	10	11,4	11,4
Disagree	16	18,2	29,5
Indecisive	34	38,6	68,2
Agree	20	22,7	90,9
Strongly Agree	8	9,1	100,0

11.4% of the respondents stated that “Strongly disagree”, 18.2% stated that they disagree “Disagree”, 38.6% remained indecisive about this issue and the remaining 31.8% said “Strongly Agree”and “Agree”, it seen that they express their opinion that the corporate ISMS processes can be operated in a healthy way. The standard deviation values of female information security staff determined as 1.040 and the mean value is 3.00. The standard deviation values of male information security staff are 1.178 and the mean value was 3.00. df 86 and significant value are .379 on independent samples based on t-test result.

6.23. Opinions about the necessity of ISO27001 Standard for information security

Percentage distribution information regarding the answers given by the Staff given in Table 6.21 to the question whether they think that the ISO27001 certification process is necessary for the effective execution of the corporation’s ISMS processes.

Table 6. 21 Question 9 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	8	9,1	9,1
Disagree	6	6,8	15,9
Indecisive	10	11,4	27,3
Agree	36	40,9	68,2
Strongly Agree	28	31,8	100,0

When the responses given analyzed, the standard deviation values of female information security staff determined as 1.166 and the mean value is 3.79. The standard deviation values of male information security staff are 1.278 and the mean value was 3.80. df 86 and significant value are .565 on independent samples based on t-test result. It seen that the positive opinion is more pressing the network. Approximately 9.1% of the respondents responded as "Strongly Disagree" and 6.8% responded as "Disagree", 11.4% were indecisive about this issue and 31.8% of the participants were "Strongly Agree". It seen that 40.9% of the respondents say “Agree” and they give a positive opinion that ISO27001 certification is necessary for the effective execution of ISMS processes.

6.24. ISO27001 opinions about ensuring external and internal security

Percentage distribution information regarding the answers given by the Staff to the question about whether the corporations having ISO27001 certification are completely safe against the information security incidents likely to come from inside or outside the corporations are given in Table 6.22. When the given responses examined, it observed that 9.1% of respondents responded as "Strongly Disagree ", 13.6% responded as "Disagree" and approximately 36.4% remained Indecisive about this matter.

Table 6. 22 Question 10 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	8	9,1	9,1
Disagree	12	13,6	22,7
Indecisive	32	36,4	59,1
Agree	26	29,5	88,6
Strongly Agree	10	11,4	100,0

On the other hand, the remaining 40.9% responded by saying "Strongly agree" and " Agree ", and it seen that having ISO27001 certification can fully protect the relevant corporation in terms of both external and internal security. The standard deviation values of female information security staff determined as 1.075 and the mean value is 3.08. The standard deviation values of male information security staff are 1.129 and the mean value was 3.30. df 86 and significant value are are .681 on independent samples based on t-test result.

6.25. Opinions on security measures taken under ISO27001

Percentage distribution information regarding the answers given by the Staff to the question whether the corporations having ISO27001 certification can protect themselves against the critical information security problems that may come from within or outside the corporation, are given in Table 6.23.

Table 6. 23 Question 11 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	6,8	6,8
Disagree	16	18,2	25,0
Indecisive	18	20,5	45,5
Agree	42	47,7	93,2
Strongly Agree	6	6,8	100,0

When the given responses examined, approximately 6.8% of respondents responded as "Strongly disagree" and 18.2% responded as "Disagree" and expressed a negative opinion on this matter. The standard deviation values of female information security staff determined as 1.125 and the mean value is 3.24. The standard deviation values of male information security staff are 1.022 and the mean value was 3.34. df 86 and significant value are .392 on independent samples based on t-test result. On the other hand, the measures taken by the corporations, which 20.5% of them are indecisive and 6.8% of them respond as "Strongly Agree", and 47.7% of them are "Agree" and have carried out by the corporations that have ISO27001 certification. It can see that they have a positive opinion that they can protect against critical information security problems that may come from outside the corporation.

6.26. Opinions of the staff in the process of transition to ISO27001 system about abandoning their habits

Corporations that have ISO27001 certification are obliged to review corporation's processes within the scope of ISMS studies, to make the necessary changes in order to re-evaluate the related processes within the framework of information security and to eliminate situations that might endanger information security. In accordance with the changes made, percentage distribution information regarding the answers given by the Staff to the question whether they have difficulties in changing the habits of the staff of the corporation is given in Table 6.24.

Table 6. 24 Question 12 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	6,8	6,8
Disagree	12	13,6	20,5
Indecisive	12	13,6	34,1
Agree	28	31,8	65,9
Strongly Agree	30	34,1	100,0

20.4% of the respondents reported negative opinions as "Strongly Disagree" and "Disagree", 13.6% remained indecisive and the remaining 65.9% said "Strongly Agree" and "Agree". Respondents, it seen that the staff of the corporation expressed their opinion that they had difficulty in changing their habits about the changes. The standard deviation values of female information security staff determined as 1.285 and the mean value is 3.61. The standard deviation values of male information security staff are 1.240 and the mean value was 3.82. df 86 and significant value are .629 on independent samples based on t-test result.

6.27. Opinions of the ISO27001 system on workload on Tech staff

The ISO27001 certification process has completed and the percentage distribution information regarding the answers given by the Staff given in Table 6.25 to the question about whether the workload on the IT staff decreases in a corporation that effectively operates the ISMS processes.

Table 6. 25 Question 13 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	30	34,1	34,1
Disagree	26	29,5	63,6
Indecisive	16	18,2	81,8
Agree	10	11,4	93,2
Strongly Agree	6	6,8	100,0

When the responses given analyzed, it seen that the opinion that the workload of informatics staff in general is dominant. 34.1% of the respondents stated that “Strongly Disagree” and 29.5% stated that they disagreed “Disagree” and the IT staff workload increased, 18.2% remained indecisive and the remaining 18.2% Likewise, it seen that the ISO27001 certification does not bring any workload to the IT staff by responding as "Strongly agree" or " Agree ". The standard deviation values of female information security staff determined as 1.242 and the mean value is 2.16. The standard deviation values of male information security staff are 1.241 and the mean value was 2.36. df 86 and significant value are .521 on independent samples based on t-test result.

6.28. Opinions on the validity of policies and procedures implemented under ISO27001

The ISO27001 certification process has completed and percentage distribution information regarding the answers given by the Staff to the question asked about the contributions of the policies and procedures implemented in the scope of ISMS processes to the corporate processes given in Table 6.26.

Table 6. 26 Question 14 - answer distribution of Information Security Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	6,8	6,8
Disagree	18	20,5	27,3
Indecisive	32	36,4	63,6
Agree	22	25,0	88,6
Strongly Agree	10	11,4	100,0

When the given responses examined, 27.3% of the respondents reported negative opinions as "Strongly Disagree" or "Disagree", 36.4% remained indecisive and 11.4% said "Strongly agree" and 25% said, "Agree" and it seen that they give a positive opinion. The standard deviation values of female information security staff determined as 1.040 and the mean value is 3.00. The standard deviation values of male information security staff are 1.117 and the mean value was 3.24. df 86 and significant value are .210 on independent samples based on t-test result.

6.29. Opinions of Tech Staff on Information Security Management System and Competencies

In this department, network specialist, system specialist software specialist, etc., working in public corporations with ISO27001. The data obtained from the technical staff will examined. 180 tech staffs working in public broadcasting corporations in four continents all around the world participated in the survey. The questionnaires distributed as 70 female and 110 male employees. In the questions asked, it planned to get the opinions of the technical staff about the corporation's ISMS and ISO27001 processes. The answers given by the participants to the survey questions examined on a question-based basis.

6.30. Opinions of the tech staff about their competencies for a healthy execution of ISMS processes

Percentage distribution information regarding the answers to the question asked whether the technical staff working in a public broadcasting corporation whose ISO27001 certification

process has been completed, is technically sufficient for the healthy execution of the corporation's ISMS processes is given in Table 6.27. When the given responses examined that, the different opinions distributed equally.

Table 6. 27 Question 1- answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	16	8,9	8,9
Disagree	56	31,1	40,0
Indecisive	16	8,9	48,9
Agree	68	37,8	86,7
Strongly Agree	24	13,3	100,0

8.9% of the respondents responded as "Strongly Disagree " and 31.1% responded as "Disagree" and gave a negative opinion on this matter, about 8.9% of them were indecisive about this and the remaining 51.1% Likewise, "Strongly agree" or "Agree" by expressing a positive answer to the question in question, that is, their technical teams think they are sufficient. The standard deviation values of female tech staff determined as 1.269 and the mean value is 3.20. The standard deviation values of male tech staff are 1.242 and the mean value was 3.13. df 178 and significant value are .959 on independent samples based on t-test result.

6.31. Opinions about the applicability of ISO27001 standard in corporate information processes

Percentage distribution information regarding the answers given to the question asked whether the policies and procedures that come with the ISO27001 standard and affect the information processes of the corporations are applicable are given in Table 6.28. When the given responses examined, it seen that the positive opinion prevails.

Table 6. 28 Question 2 - answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	4	2,2	2,2
Disagree	14	7,8	10,0
Indecisive	36	20,0	30,0
Agree	102	56,7	86,7
Strongly Agree	24	13,3	100,0

It seen that 10% of the participants' stated negative opinions as "Strongly Disagree" or "Disagree", and 20% of them remained indecisive in this regard. On the other hand, "Strongly Agree" of the remaining 13.3% and It determined that 56.7% of the respondents responded positively as "Agree", that is, they stated that ISO27001 standard is applicable in corporate processes. The standard deviation values of female tech staff determined as .922 and the mean value is 3.70. The standard deviation values of male tech staff are .847 and the mean value was 3.72. df 178 and significant value are .509 on independent samples based on t-test result.

6.32. Opinions on the training / training requirement related to ISO27001

Percentage distribution information regarding the answers given to the question asked whether there is a need for training related to ISO27001 as well as the duties of technical staff working in public broadcasting corporations with ISO27001 standard given in Table 6.29.

Table 6. 29 Question 3 - answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	8	4,4	4,4
Disagree	10	5,6	10,0
Indecisive	10	5,6	15,6
Agree	84	46,7	62,2
Strongly Agree	68	37,8	100,0

When the given responses examined, positive opinion prevails. The standard deviation values of female tech staff determined as 1.067 and the mean value is 4.14. The standard deviation values of male tech staff are 1.004 and the mean value was 4.04. df 178 and significant value are .339 on independent samples based on t-test result. It can see that 10% of the participants stated negative opinions as "Strongly Disagree" or "Disagree", and 5.6% of them remained indecisive in this regard. On the other hand, it seen that 37.8% of them express their opinions as "Strongly agree" and 46.7% of them say "Agree". It determined that the majority of the Tech Staff stated that it would be beneficial to receive training on ISO27001.

6.33. Opinions about the benefits of ISO27001 processes to Tech Staff

In this question addressed to the technical staff working in public broadcasting corporations with ISO27001 standard, it was trying to understand whether the ISO27001 standard contributed positively in terms of the related people's ability to carry out their duties more effectively and healthily. Percentage distribution information of the given answers given in Table 6.30. When the answers given examined, and seen positive opinion prevails.

Table 6. 30 Question 4 - answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	3,3	3,3
Disagree	18	10,0	13,3
Indecisive	46	25,6	38,9
Agree	84	46,7	85,6
Strongly Agree	26	14,4	100,0

It observed that 3.3% of the participants stated negative opinions as "Strongly Disagree" and 10% of them stated "Disagree". On the other hand, 25.6% of them are indecisive on this matter, while the remaining 61.1% of them respond positively to the question as "Strongly agree" or "Agree ". It has been determined that it will be beneficial in terms of execution in a way. The standard deviation values of female tech staff determined as 1.008 and the mean value is 3.64. The standard deviation values of male tech staff are .944 and the mean value was 3.55. df 178 and significant value are .805 on independent samples based on t-test result.

6.34. Opinions about the contributions provided by the measures taken under ISO27001

Percentage distribution information regarding the answers given to the question asked whether the public broadcastıng corporations with ISMS have completed the ISO27001 standardization process and whether there is a decrease in the information security incidents compared to the previous periods given in Table 6.31.

Table 6. 31 Question 5 - answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	3,3	3,3
Disagree	10	5,6	8,9
Indecisive	30	16,7	25,6
Agree	98	54,4	80,0
Strongly Agree	36	20,0	100,0

When the given responses examined, the positive opinion prevails. The standard deviation values of female tech staff determined as 1.002 and the mean value is 3.84. The standard deviation values of male tech staff are .883 and the mean value was 3.81. df 178 and significant value are .369 on independent samples based on t-test result. Participants, 8.9% reported negative opinions as "Strongly Disagree" or "Disagree", 16.7% remained indecisive about this issue, and on the other hand, 20% had “Strongly Agree", 54.4% it observed that a small percentage of respondents positively responded to the question "Agree", that is, they reported that information security incidents decreased after ISO27001.

6.35. Opinions of the ISO27001 Standard on the positive contributions to the security of the developed corporate practices

Percentage distribution information regarding the answers to the question asked whether the ISO27001 standardization process contributes positively to the security of corporation’s applications developed in public broadcasting corporations with ISMS given in Table 6.32.

Table 6. 32 Question 6 - answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	4	2,2	2,2
Disagree	10	5,6	7,8
Indecisive	22	12,2	20,0
Agree	106	58,9	78,9
Strongly Agree	38	21,1	100,0

When the given responses examined, the positive opinion prevails. Approximately 2.2% of the participants “Strongly Disagree”, It observed that 5.6% of them stated negative opinions as "Disagree" and 12.2% of them were indecisive on this matter. On the other hand, it determined that the remaining 80% of the total responded positively to the question in question by saying “Strongly Agree" or "Agree". The standard deviation values of female tech staff determined as .953 and the mean value is 3.93. The standard deviation values of male tech staff are .812 and the mean value was 3.90. df 178 and significant value are .297 on independent samples based on t-test result.

6.36. Opinions about ISO27001's contribution to the reduction of information security violation incidents

In public broadcastıng corporations with ISO27001 certificate, percentage distribution information regarding the answers to the question asked whether the standardization process contributes positively to the reduction of Info-Sec violation incidents given in Table 6.33.

Table 6. 33 Question 7 - answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	4	2,2	2,2
Disagree	10	5,6	7,8
Indecisive	40	22,2	30,0
Agree	104	57,8	87,8
Strongly Agree	22	12,2	100,0

When the given responses examined, the positive opinion prevails. The standard deviation values of female tech staff determined as .903 and the mean value is 3.71. The standard deviation values of male tech staff are .789 and the mean value was 3.73. df 178 and significant value are .299 on independent samples based on t-test result. It observed that 7.8% of the participants reported negative opinions as "Strongly Disagree" or "Disagree", and 22.2% remained indecisive in this regard. It found that the remaining 70% of the total responded by saying "Strongly Agree" or " Agree " and that ISO27001 standardization contributed positively to the reduction of information security incidents.

6.37. Opinions of ISO27001 on the applicability of regulatory and preventive activities

Information security vulnerabilities identified in the scope of risk management and audit processes carried out within the scope of ISO27001 compliance processes and ISMS studies should determined and the actions to be taken afterwards. Percentage distribution information regarding the answers to the question asked whether regulatory and preventive activities, which is one of the aforementioned transactions, provide a beneficial contribution to the relevant corporation in the information security management process, are given in Table 6.34.

Table 6. 34 Question 8 - answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	4	2,2	2,2
Disagree	12	6,7	8,9
Indecisive	4	2,2	11,1
Agree	104	57,8	68,9
Strongly Agree	56	31,1	100,0

When the given responses examined, the positive opinion is significantly dominant. 8.9% of the participants reported negative opinions as “Strongly Disagree" or "Disagree", It observed that 2.2% of them remained indecisive in this regard. On the other hand, it seen that 31.1% of them stated, “Strongly agree”, 57.8% of them said “Agree”, and they thought that regulatory and preventive activities contributed positively. The standard deviation values of female tech staff determined as .971 and the mean value is 4.11. The standard deviation values of male tech staff are .808 and the mean value was 4.09. df 178 and significant value are .113 on independent samples based on t-test result.

6.38. Opinions on the contributions of security measures taken under ISO27001

Percentage distribution information regarding the answers to the question asked whether there would be less problems on the system because of increasing the measures taken within the scope of ISO27001 compliance processes and ISMS studies and further tightening of the system given in Table 6.35.

Table 6. 35 Question 9 - answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	2	1,1	1,1
Disagree	16	8,9	10,0
Indecisive	26	14,4	24,4
Agree	86	47,8	72,2
Strongly Agree	50	27,8	100,0

When the given responses examined, the standard deviation values of female tech staff determined as .963 and the mean value is 4.00. The standard deviation values of male tech staff are .920 and the mean value was 3.87. df 178 and significant value are .815 on independent samples based on t-test result. The positive opinion prevails. 10% of the respondents reported negative opinions as "Strongly Disagree" or "Disagree", 14.4% of them were indecisive about this issue, and 27.8% of them agree “Strongly Agree” and 27.8% stated “Agree, said. They thought they had contributed positively to less information security incidents after the mentioned measures were increased.

6.39. Opinions of ISO27001 on the predetermination of possible risks

Percentage distribution information regarding the answers given to the question asked whether corporate information security risks could detect before realization in the case of ISO27001 compliance processes and control substances provided in Table 6.36.

Table 6. 36 Question 10 - answer distribution of Tech Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	6	3,3	3,3
Disagree	8	4,4	7,8
Indecisive	24	13,3	21,1
Agree	100	55,6	76,7
Strongly Agree	42	23,3	100,0

When the given responses examined, the positive opinion prevails. The standard deviation values of female tech staff determined as .997 and the mean value is 3.93. The standard deviation values of male tech staff are .867 and the mean value was 3.90. df 178 and significant value are .433 on independent samples based on t-test result. Approximately 7.7% of the respondents reported negative opinions as "Strongly Disagree" and "Disagree", 13.3%. Remained indecisive about this issue, 23.3% said "Strongly agree" and 55.6% and responded as "Agree" and it has seen that 78.9% gave a positive opinion to this question. From this, it has seen that a positive opinion has expressed as a positive contribution to the determination of information security risks in advance.

6.40. Opinions of Staff's About Information Security Management System and Awareness Training

In this section, the data obtained from the staff working in public broadcastıng corporations having ISO27001 will examined. It was trying to inform about the questions asked to the staff and the awareness trainings of the staff within the scope of the ISMS studies and their general opinions about the system. 658 staff working in public broadcasting corporations in 4 continents all around the world participated in the survey. The questionnaires distributed as 196 female and 462 male employees. The answers given by the participants to the survey questions examined on a question basis below.

6.41. Opinions of the duration of the information training given about ISO27001

One of the most important processes of ISO27001 is the establishment of corporate information security awareness. In this context, various information trainings given to the staff of the corporation in line with their duties. Percentage distribution information regarding the answers to the question asked whether the duration of the trainings given is sufficient or not given in Table 6.37.

Table 6. 37 Question 1 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	26	4,0	4,0
Disagree	80	12,2	16,1
Indecisive	122	18,5	34,7
Agree	362	55,0	89,7
Strongly Agree	68	10,3	100,0

When the given responses examined, the positive opinion prevails. The standard deviation values of female other staff determined as 1.035 and the mean value is 3.54. The standard deviation values of male other staff are .938 and the mean value was 3.56. df 656 and significant value are .105 on independent samples based on t-test result. 16.2% of the respondents responded as "Strongly Disagree" or "Disagree" and 18.5% remained indecisive about this issue, and the remaining 65.3% of the total questioned. It observed that he responded positively as “Strongly agree" or "Agree", that is, and he expressed his opinion that the duration of the training provided was sufficient.

6.42. Opinions of the content of the information trainings about ISO27001

Percentage distribution information regarding the answers to the question asked whether the content of the trainings given to the staff of the corporation within the scope of ISMS is sufficient is given in Table 6.38.

Table 6. 38 Question 2 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	16	2,4	2,4
Disagree	86	13,1	15,5
Indecisive	156	23,7	39,2
Agree	324	49,2	88,4
Strongly Agree	76	11,6	100,0

When the given responses examined, the positive opinion prevails. The standard deviation values of female other staff determined as 1.004 and the mean value is 3.54. The standard deviation values of male other staff are .916 and the mean value was 3.55. df 656 and significant value are .119 on independent samples based on t-test result. It observed that 2.4% of the respondents stated “Strongly Disagree”, 13.1% of them expressed negative opinions as “Disagree” and 23.7% of them were indecisive on this matter. On the other hand, it observed that 11.6% of the respondents answered “Strongly Agree” and 49.2% responded as “Agree” and positively responded to the question in question, that is, the content of the training provided was sufficient.

6.43. Opinions about the adequacy of the materials given during the awareness trainings carried out under ISO27001

Percentage distribution information regarding the answers given to the question asked whether the materials and samples given during the trainings given to the staff of the ISMS are sufficient or up-to-date are given in Table 6.39. When the given responses examined, it seen that the positive opinion prevails.

Table 6. 39 Question 3 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	24	3,6	3,6
Disagree	60	9,1	12,8
Indecisive	198	30,1	42,9
Agree	318	48,3	91,2
Strongly Agree	58	8,8	100,0

3.6% of the respondents stated that “Strongly disagree”, 9.1% said “Disagree” and 30.1% remained indecisive about this issue and the remaining 57.1% said, “It found that he definitely answered” Strongly Agree” and “Agree” positively to the question in question, that is, the materials and examples given during the trainings were sufficient. The standard deviation values of female other staff determined as .958 and the mean value is 3.50. The standard deviation values of male other staff are .890 and the mean value was 3.49. df 656 and significant value are. .365 on independent samples based on t-test result.

6.44. Opinions about the benefits of information security awareness training

Percentage distribution information regarding the answers given to the question asked whether the trainings given to the staff of the corporation within the scope of ISMS are useful in creating information security awareness and having information about current threats given in Table 6.40.

Table 6. 40 Question 4 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	20	3,0	3,0
Disagree	50	7,6	10,6
Indecisive	108	16,4	27,1
Agree	336	51,1	78,1
Strongly Agree	144	21,9	100,0

When the given responses examined, the positive opinion prevails. The standard deviation values of female tech other determined as 1.016 and the mean value is 3.80. The standard deviation values of male tech other are .940 and the mean value was 3.82. df 656 and significant value are .202 on independent samples based on t-test result. A total of 10.6% of the respondents reported negative opinions as " Strongly Disagree" and "Disagree", 16.4% remained indecisive about this issue, 21.9% of them were "Strongly Agree", 51.1% It observed that the part of " responded positively to the question in question as “Agree”, that is, 73% of the total stated that the trainings were beneficial for them.

6.45. Opinions about the applicability of the information given within the scope of awareness training in terms of corporation processes

Percentage distribution information regarding the answers given to the question asked whether the information given in awareness trainings within the scope of ISMS processes is applicable in terms of corporation processes given in Table 6.41.

Table 6. 41 Question 5 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%)Total Percentage
Strongly Disagree	8	1,2	1,2
Disagree	54	8,2	9,4
Indecisive	160	24,3	33,7
Agree	340	51,7	85,4
Strongly Agree	96	14,6	100,0

When the given responses examined, the positive opinion prevails. The standard deviation values of female other staff determined as .896 and the mean value is 3.71. The standard deviation values of male other staff are .845 and the mean value was 3.70. df 656 and significant value are .405 on independent samples based on t-test result.A total of 9.4% of the participants reported negative opinions as "Strongly Disagree" or "Disagree", and approximately 24.3% of them were indecisive on this matter, 14.6% of them were "Strongly Agree", It seen that 51.7% of the respondents positively answered the question as "Agree", that is the information given in the trainings at a rate of 66.3% is applicable in terms of corporation processes.

6.46. Opinions on the content of awareness education

Percentage distribution information regarding the answers to the question asked whether the content should be important rather than the duration of the awareness trainings within the scope of ISMS processes given in Table 6.42.

Table 6. 42 Question 6 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	20	3,0	3,0
Disagree	22	3,3	6,4
Indecisive	88	13,4	19,8
Agree	286	43,5	63,2
Strongly Agree	242	36,8	100,0

When the given responses examined, the standard deviation values of female other staff determined as 1.029 and the mean value is 4.05. The standard deviation values of male other staff are .917 and the mean value was 4.09. df 656 and significant value are .133 on independent samples based on t-test result. Important majority gives a positive opinion. 6.3% of the participants expressed negative opinions as “Strongly Disagree" or "Disagree". 13.4% of them were indecisive on this issue, and 80.3% of them totally agree, "Strongly agree" or "Agree" It observed that they responded positively to the question in question, that is, they expressed their opinion that their content was important rather than the duration of their awareness training.

6.47. Opinions about the method of awareness education

Percentage distribution information regarding the answers given to the question asked whether the awareness trainings within the scope of ISMS processes are sufficient, only through slides given in Table 6.43.

Table 6. 43 Question 7 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	76	11,6	11,6
Disagree	216	32,8	44,4
Indecisive	178	27,1	71,4
Agree	158	24,0	95,4
Strongly Agree	30	4,6	100,0

When the answers given analyzed, it seen that the negative opinion is dominant. The standard deviation values of female other staff determined as 1.109 and the mean value is 2.81. The standard deviation values of male other staff are 1.065 and the mean value was 2.76. df 656 and significant value are .509 on independent samples based on t-test result. 11.6% of the participants stated that “Strongly disagree”, 32.8% of them expressed negative opinion as “disagree”, that the slides were not sufficient for effective training, 27.1% of them were indecisive about this issue. The remaining 28.6% of them found to have responded positively to the question in question, that is, the opinion that the method of education made on the slides was sufficient.

6.48. Opinions of the corporation that gives awareness training about its qualifications

Percentage distribution information regarding the answers to the question asked whether the training companies or trainers transfer the experiences gained from other corporations to the staff during the awareness trainings within the scope of ISMS processes given in Table 6.44.

Table 6. 44 Question 8 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	30	4,6	4,6
Disagree	74	11,2	15,8
Indecisive	204	31,0	46,8
Agree	296	45,0	91,8
Strongly Agree	54	8,2	100,0

When the given responses examined, the positive opinions are dominant. The standard deviation values of female other staff determined as 1.016 and the mean value is 3.41. The standard deviation values of male other staff are .924 and the mean value was 3.41. df 656 and significant value are .124 on independent samples based on t-test result. It seen that 15.8% of the participants reported negative opinions about this issue as “Strongly Disagree" or "Disagree". It determined that 31% of them remained indecisive in this regard. On the other hand, 8.2% of the participants responded positively to the question “Strongly Agree”, 45% of them agree “Agree”, and stated that the company or trainers who trained conveyed the most up-to-date information and experiences they received from other corporations. It observed.

6.49. Opinions about the effects of security measures taken within the scope of ISMS on powers

Within the scope of ISMS processes, Percentage distribution information regarding the answers to the question asked whether the measures taken and the restrictions on the information systems limit the staff’s powers excessively given in Table 6.45.

Table 6. 45 Question 9 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	62	9,4	9,4
Disagree	218	33,1	42,6
Indecisive	180	27,4	69,9
Agree	164	24,9	94,8
Strongly Agree	34	5,2	100,0

When the given responses examined, the standard deviation values of female other staff determined as 1.101 and the mean value is 2.87. The standard deviation values of male other staff are 1.053 and the mean value was 2.82. df 656 and significant value are .485 on independent samples based on t-test result. It observed that 9.4% of respondents responded as "Strongly Disagree" and 33.1% responded as "Disagree" and that they expressed an opinion that the authorities were not restricted excessively. It observed that 27.4% of them remained indecisive in this regard. On the other hand, the remaining 30.1% of the total responded as "Strongly Agree" or "Agree" and positively responded to the question in question, meaning that their powers were extremely restricted.

6.50. Opinions about whether corporate ISMS managed well or not

In public broadcasting corporations whose ISO27001 certification process has completed, percentage distribution information regarding the answers to the question asked whether the ISMS processes have carried out well given in Table 6.46.

Table 6. 46 Question 10 - answer distribution of Other Staff survey

	Number of People	(%) Percentage	(%) Total Percentage
Strongly Disagree	16	2,4	2,4
Disagree	38	5,8	8,2
Indecisive	178	27,1	35,3
Agree	318	48,3	83,6
Strongly Agree	108	16,4	100,0

When the given responses examined, the standard deviation values of female other staff determined as .952 and the mean value is 3.70. The standard deviation values of male other staff are .869 and the mean value was 3.71. df 656 and significant value are .209 on independent samples based on t-test result. It observed that 8.2% of the respondents responded as “Strongly Disagree" or "Disagree" and gave a negative opinion on this issue, and 27.1% remained indecisive on this matter. On the other hand, it observed that 16.4% of them responded as “Strongly Agree” and 48.3% of them responded as “Agree” and positively. As a result, it observed that 64.7% responded positively to the question in question, and expressed their opinion that the conducted ISMS well managed.

In addition to all research, particularly when viewed in the value of the public broadcasting corporation in Turkey that for 145 employees who 53 females and 92 males. When the given responses examined, general mean examined 3,87. the mean value is 3.77 and df 15 for management, the mean value is 3.86 and df 8 for Information Security Staff, the mean value is 4.44 and df 16 for Tech Staff, the mean value is 3.77 and df 15 for Other Staff. As indicated by this research, especially it has seen as ISO27001 supported by the public broadcasting corporation in Turkey.

6.51. Reverse Analysis

Implementation of a comprehensive standard such as ISO 27001 impact company staff in a variety of ways and the survey designed to query different classes of employees in terms of the factors relevant to them. Each question pertained to employee views regarding the implementation for the relevant aspect. For most questions, a score of one implies a strongly negative view, while five suggests a strongly positive view. For questions where the implications reversed, the scores reversed for the analyses so that a higher score again implied greater positive perception. The overall view of an employee, incorporating the various factors, can inferred from their average score on the quiz.

6.51.1. Overall perceptions

Table 6.47. presents the percentage distribution of average employee score for the survey where each row includes responses with average up to, and including, the value indicated.

Table 6. 47 Percentage Distribution of Employee Average Survey Score

	Management	**Security Team**	**IT Staff**	**Other Staff**
Observations	156	88	180	658
Range	Percentage of Responses			
1	1.28	4.55	1.11	1.22
1.25	0.00	2.27	1.11	1.22
1.5	3.21	2.27	1.11	1.22
1.75	3.21	0.00	0.00	0.91
2	1.28	6.82	4.44	4.86
2.25	0.00	4.55	0.00	1.22
2.5	1.92	6.82	2.22	4.86
2.75	1.92	2.27	0.00	0.61
3	3.85	4.55	5.56	17.63
3.25	3.85	9.09	5.56	1.52
3.5	2.56	15.91	8.89	7.60
3.75	14.10	6.82	8.89	3.95
4	7.69	2.27	23.33	24.62
4.25	10.26	13.64	10.00	12.16
4.5	11.54	9.09	7.78	6.08
4.75	15.38	2.27	6.67	2.13
5	17.95	6.82	13.33	8.21

Figures 6.1. - 6.4. present bar charts for absolute numbers of responses in the various ranges, by staff type.

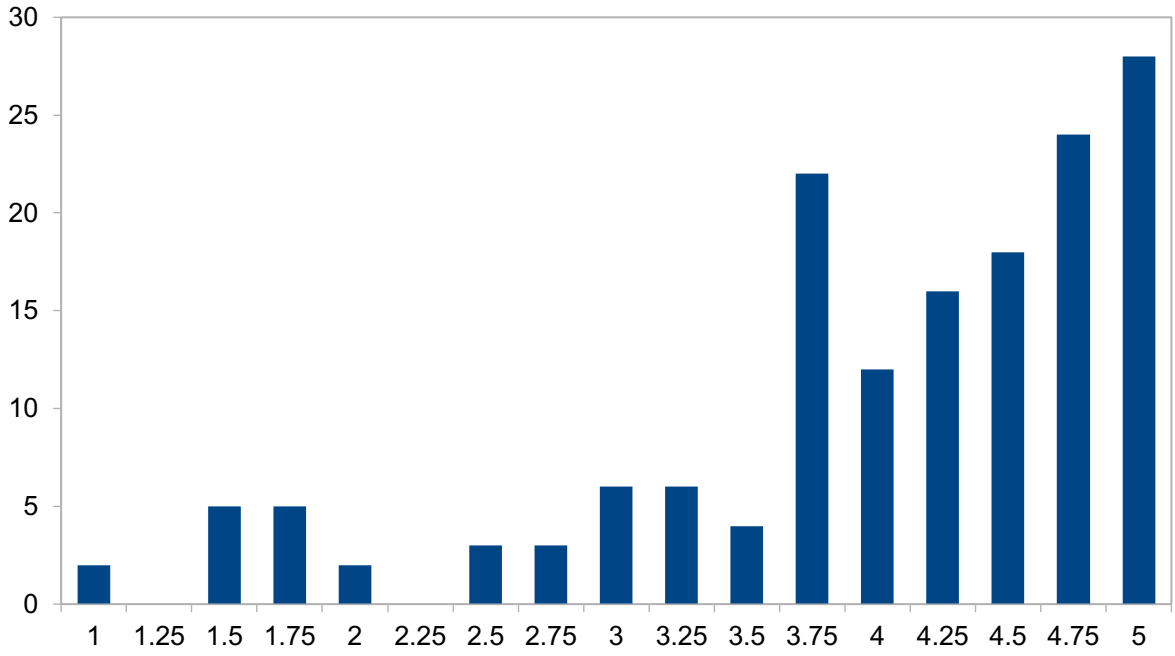

Figure 6. 1 Distribution of Responses by Average Survey Score for Management

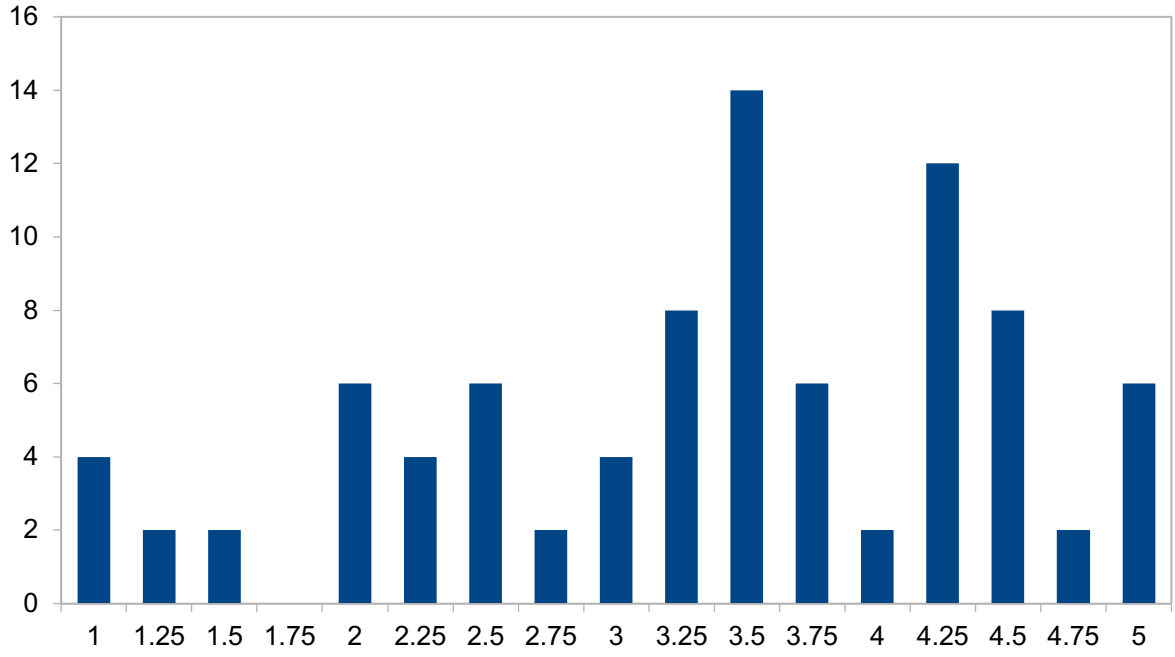

Figure 6. 2 Distribution of Responses by Average Survey Score for Information Security Team

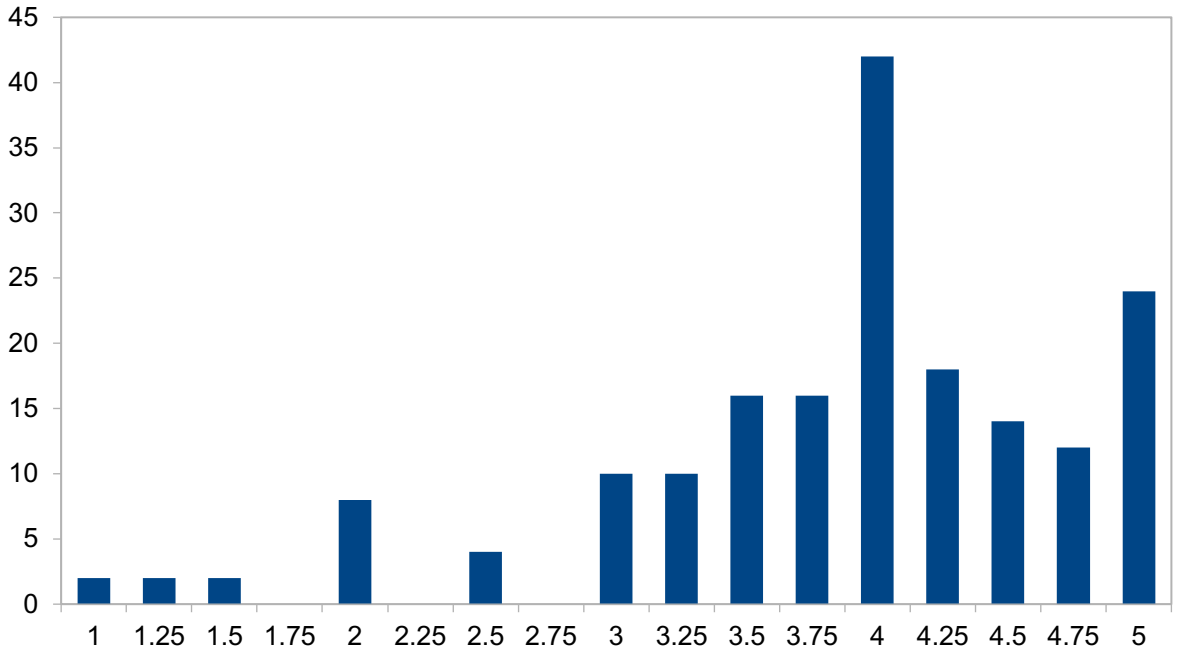

Figure 6. 3 Distribution of Responses by Average Survey Score for Information Technology Staff

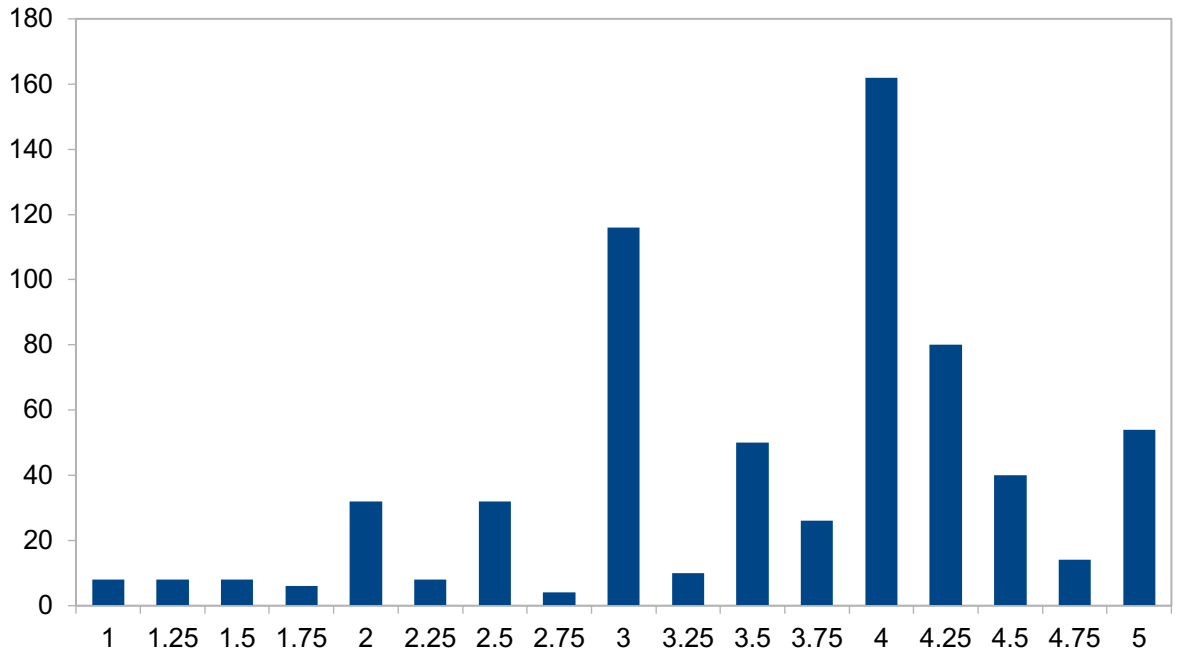

Figure 6. 4 Distribution of Responses by Average Survey Score for Other Staff

Table 6.48. provides the statistics for the distributions of Figures 6.1.- 6.4. All calculated means are greater than 3, the value which would indicate an overall neutral viewpoint. Two-tailed t-tests confirm the means to be statistically different from 3 at the 1% level, except for the Information Security Team for which the significance was at the 5% level.

Table 6. 48 Statistics for Distributions of Average Survey Scores

	Management	**Security Team**	**Tech Staff**	**Other Staff**
Min	1	1	1	1
Max	5	5	5	5
Median	4.08	3.36	4.00	3.80
Mean	3.92	3.26	3.79	3.49
T-Value (m=3)	11.598	2.282	11.883	13.846
Significance	***	**	***	***

Significance levels ***, **, * indicate $p \leq 0.01$, $p \leq 0.05$, and $p \leq 0.1$ respectively, in comparison with critical t-values for two-tailed tests.

While Table 6.48. suggests Management to hold the most positive overall view towards ISO 27001 implementation, followed by Information Technology Staff and then Other Staff, with the Information Security Team being the least positive; Table 6.49, which presents pairwise comparison of the means of the distributions using two-tailed t-tests without assuming equality of variance, indicates that the mean of the distribution for Management responses is not significantly different from that of Information Technology Staff, and the mean for Information Security Team differs from that of Other Staff only at 10% significance.

Table 6. 49 p-Values for Comparisons of Distribution Means

	Management	**Security Team**	**Tech Staff**
Security Team	< .0001***		
Tech Staff	.2334	.0001***	
Other Staff	< .0001***	.0586*	< .0001***

Thus, Management and Information Technology Staff appear to have a more positive overall perspective towards ISO 27000 implementation than Information Security Team as well as Other Staff, even as all categories show a positive response overall.

6.51.2. Individual Questions

Tables 6.50. - 6.53. present the mean, median and mode for responses to individual questions, by personnel category.

Table 6. 50 Response Summary for Management Questions

Question	Mean	Median	Mode
1	4.35	5	5
2	4.19	4	5
3	4.14	4	5
4	4.21	4	5
5	4.32	5	5
6	4.49	5	5
7	3.99	4	4
8	3.00	3	3
9	3.08	3	4
10	3.88	4	4
11	3.78	4	4
12	3.56	4	4

Table 6. 51 Response Summary for Information Security Team Questions

Question	Mean	Median	Mode
1	3.77	4	4
2	2.98	3	3
3	4.30	5	5
4	3.18	3	4
5	2.91	3	2
6	3.25	3	3
7	2.84	3	2
8	3.00	3	3
9	3.80	4	4
10	3.20	3	3
11	3.30	4	4
12	3.73	4	5
13	2.27	2	1
14	3.14	3	3

Table 6. 52 Response Summary for Information Technology Staff Questions

Question	Mean	Median	Mode
1	3.16	4	4
2	3.71	4	4
3	4.08	4	4
4	3.59	4	4
5	3.82	4	4
6	3.91	4	4
7	3.72	4	4
8	4.10	4	4
9	3.92	4	4
10	3.91	4	4

Table 6. 53 Response Summary for Other Staff Questions

Question	Mean	Median	Mode
1	3.56	4	4
2	3.54	4	4
3	3.50	4	4
4	3.81	4	4
5	3.70	4	4
6	4.08	4	4
7	2.77	3	2
8	3.41	4	4
9	2.83	3	2
10	3.71	4	4

CONCLUSIONS AND RECOMMENDATIONS

Since there are very few analyzes with this approach in the literature, I think that the analysis I have made will contribute to the literature. It is evident that the corporation information security management or the compliance of these systems with any standardization does not mean that information security ensured in corporate processes. It is of great importance that the corporation's management owns the established systems and the staff of the corporations at all levels. For this reason, it expected that one of the indispensable elements of ISO27001 compliance processes in particular is to prove the existence of a strong will behind the system and to prove that this will have done the necessary work to carry out the related processes effectively. On the other hand, it is also important to understand and adopt the ISMS processes established by both technical staff and other staff carrying out operational processes. In this context, ISO27001 necessitates a set of informing and awareness raising activities for all levels of staff.

Information security, human, technology and process are the three basic elements, and failure of any of these three elements means that information security cannot ensured. These three elements must keep up-to-date due to technological developments and changes. No matter how technology and process elements are flawlessly and up-to-date and positioned. Human element does not make sense unless it is up to date in the face of developments and changes. For this reason, due to the human element, the effectiveness and continuity of corporate information security management constantly questioned and should questioned.

In this thesis, a research conducted on the staff of the corporation, which is the most important element of information security. In this context, public broadcasting corporations that have ISO27001 certificate examined through various groups of staff from different levels and duties. Findings and results obtained from the review presented below.

When the responses given by the executive levels of the corporations analyzed, it seen that the positive view regarding ISO27001 standardization processes and corporation's contributions in general is dominant. It seen that the opinions that ISO27001 is necessary for the corporations in general and that it is an indicator of corporation's reputation and trust prevail. On the other hand, it seen that the executive level has expressed a positive opinion on the fact that ISO27001

contributes to the achievement of corporate information security targets and to increase the efficiency and effectiveness of the corporate policies developed within the scope of ISMS. At the same time, ISO27001 thought to have contributed positively in creating corporate information security awareness.

The opinion that the management support is of great importance in terms of fulfilling the requirements of ISO27001 certification process and ISMS and at this point, the duties falling on the management level are one of the important results obtained from the obtained data. On the other hand, consensus among managers on the issue that managers should be privileged within the scope of the authorization policies that came with ISO27001 and whether the related ISMS processes bring additional workload.

It seems that there is no. It observed that the number of managers who think that they bring additional workload and the number of managers who think they do not and who should think they should have privileges are close to each other. In general terms, it seen that the management level found the ISO27001 processes positive and thought that the process positively contributes to corporate information security.

When the responses given by the Information Security Staff, which created to manage and develop ISO27001 compliance processes, analyzed, it seen that the Staff think that ISO27001 is necessary to ensure corporate information security. In line with this view, it has seen that the opinion that ISO27001 is beneficial in terms of protecting the corporation against internal and external threats has reported. It has observed that ISO27001 compliance processes are difficult to manage with the human resources in the numerical sense of the corporation and that professional consultancy support is required from outside the corporation. Nevertheless, it seen that the human resources of the corporations are insufficient in terms of experience and knowledge and they think that information security staff should receive training in order to manage the processes in a healthy way. Nevertheless, a consensus on whether the ISMS team to be established should consist of IT staff.

It seen that the number of opposing views and indecisive ones is close to each other. It seen that, within the scope of ISO27001 compliance processes, it is possible to work harmoniously with

corporation's staff, but that there is not enough support in the management of corporate information security risk processes.

It has also observed that the corporation's staff outweighed the difficulties in adapting to the process changes coming with ISO27001 as they had difficulties in abandoning their old habits. From the perspective of IT staff, it seen that the return to the question of whether ISO27001 reduces the workload or not, the workload is not decreasing. In terms, ISMS teams have seen that they think that they are not sufficient in terms of experience, numerically and they need training, and that they do not get enough support in terms of working with staff, especially in risk studies. Although opinions expressed that ISO27001 is necessary for the corporation, it seen that opinions expressed that workload did not decrease.

When the responses of the technical staff in charge of the management of the information systems and technical infrastructure in charge of the corporations and producing solutions in line with the corporate needs examined, it seen that there is no consensus on whether the technical staff responsible is technically and quantitatively. The reason for this is that the technical team in different public broadcastıng corporations differ in the number of competencies. The view that ISO27001 is applicable on corporate technical processes seems to outweigh. It also seen in their technical teams that they had an opinion about training needs regarding ISO27001 processes. On the other hand, it observed that the opinions that the ISO27001 compliance process positively contributed to the security of the corporate applications developed by the technical team. At the same time, in line with the answers given, it can evaluate that there is a significant decrease in the number of information security incidents experienced with the transition to ISO27001.

When the general awareness levels of the staff of the corporation, the trainings they have received. Their opinions about ISMS tried to learn, when the responses received in this section examined, they are generally satisfied with the awareness trainings they have received, their content and duration are sufficient, but only on slides.

It observed that the trainings were not sufficient. At the same time, it has observed that educational firms or trainers give opinions that the information they provide in education includes current information and other corporations. On the other hand, the answer to the question as to whether the powers of the staff are excessively restricted or not has a significant

difference between the different opinions where the positive and negative answers are close to each other.

As a result, because of the examination made in terms of staff, it found that the Information security awareness trainings given to the staff of the corporation found positive in terms of content, duration and benefit. On the other hand, it also seen that there are opinions that the controls and authority restrictions applied by the staff are too high. In general, it seen that there was a trust against the system established by the staff, that the staff of the corporation adopted ISO27001 and that they thought that the ISMS processes managed effectively in their corporations.

Recommendations, suggestions developed based on the findings obtained from the questionnaire studies applied in this section given below under different headings. Recommendations for the management:

It observed that the management level did not have a great deal of information about their responsibilities. For this, special directions can made to the management level with Cyber Action Plans or circulars.

A study can conducted to measure the awareness and ownership levels appropriate for the management level.

The importance of information security studies can transfer to the management level in more detail, thus increasing the ownership levels.

Risk studies can be included in order to better perceive the necessity of the established ISMS by the management level.

A study can carried out with the managers of public broadcasting corporations to establish a common Information security installation directive.

Together with the managers of the public broadcasting corporations, special risks and opportunities can studied for broadcasters.

Recommendations to the information security team;

More attention should pay to the installation of information security teams. The responsibilities of the established team should clearly determine and the level of education should select among the appropriate staff.

The number of information security staff considered to insufficient. In this regard, staff should determine in direct proportion to the number of staffs in the corporation.

Although the staffs introduced to the personnel of the corporations in awareness training, it seen that the majority of the personnel do not recognize the staffs. It is possible to provide information about this more effectively.

In order to facilitate the work of staff, assignments can made by senior management from all units and corporation staff can ensured to own the ISMS management processes.

It has been determined that information security staffs are not able to work in harmony with corporate personnel in corporate risk studies. Providing training to the staff of the corporation assigned in this process on risk determination and processing can contribute more effectively manage of the process.

Studies can carry out to increase ownership levels of information security staff.

It has observed that information security staff find themselves inadequate and provide opinions regarding their training needs. In this context, it can ensure to determine all the training content to needed and to receive all training before assignment.

It observed that information security staff should not be entirely composed of information technology staff. Assignments can also made to staff outside of the IT staff.

By making a more detailed study of information security staff, it is possible to clarify the job descriptions of the staff and even to make team-specific staff work.

Information security staff ' job descriptions can be supported by cyber action plans or guidelines.

Recommendations for the tech staff;

It observed that the opinion that the number of technical staffs were insufficient expressed. In this context, the number of technical staffs should increase.

It seen that the level of knowledge of technical teams about ISO27001 is not sufficient, but they still own the process. The reason for this may be that the management of operational processes contributes positively to the system. For this reason, basic information security trainings can give due to the increase of awareness of the technical team about ISO27001.

Software teams can give more attention to information security issues during their studies. In this context, awareness levels can increase by providing entry-level trainings such as secure code development, basic ISMS, and basic network security.

Active participation of software teams can achieve in penetration tests conducted within the scope of information security.

Recommendations for the Other Staff;

It thought that it would be more beneficial to give awareness training on practical examples rather than presentations.

It has observed that the duration and content of the awareness trainings are sufficient, but that the content is the same in every education affects the desire to participate negatively. For this reason, the training times are as short as possible and the training content can plan by changing each training.

The restrictions made in line with the measures taken within the scope of information security found to be excessive by some of the personnel. This thought to relate to the awareness levels of the staff. In awareness trainings, it is possible to focus on information on authorizations.

Recommendations for the future research;

Survey participation rates found to be higher in face-to-face surveys. In order to increase the participation rate in similar studies likely to carry out, questionnaires can made face-to-face as well as electronic environment.

Work can reduce to a special management level and deepened.

It concluded that there are differences between ISO and ISO27001 between senior management and lower level management. The reasons for this in subsequent studies can investigated.

It should not forget that it is difficult to obtain survey application permits especially in public broadcastıng corporations and a careful study is required.

A more in-depth study can carry out by reducing the work done to public broadcasters.

The next studies can examine in terms of consultancy firms and trainers.

The relationship between legislation and ISO27001 can examined from a legal point of view, across the public broadcasting corporations or in particular of any public broadcasting corporations.

Common or diverging aspects can investigated in public public broadcasting corporations between Personal Data Protection Law and ISO27001.

Data stream and privacy protection with machine learning in public broadcasting is planing as a doctoral project in the future.

REFERENCES

Achmadi, D., Suryanto Y. & Ramli K. (2018). *On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center*. In 2018 International Workshop on Big Data and Information Security (IWBIS). Jakarta, Indonesia.

Akay, İ.G. (2014). *Bilgi güvenliği yönetim sistemleri: Bilgi güvenliği uygulama mülakatları*, Bilecik Şey Edebali Üniversitesi Sosyal Bilimler Enstitüsü, Bilecik

Almeida, L. & Respício, A. (2018). *Decision support for selecting information security controls*. Journal of Decision Systems. 27(sup1), 173-180.

Al-Aqeeli, S., Al-Rodhaan M., & Tian Y. (2017). *Privacy preserving risk mitigation strategy for access control in e-healthcare systems.* in 2017 International Conference on Informatics, Health & Technology (ICIHT). Riyadh, KSA.

Arce, I. (2003). *The weakest link revisited* [information security]. IEEE Security & Privacy. 1(2), 72-76.

Asosheh, A., Hajinazari P., & Khodkari H. (2013). *A practical implementation of ISMS. in 7th International Conference on e-Commerce in Developing Countries: with focus on e-Security*. 2013 of Conference. Kish Island, Iran.

Aydoğmuş, E. (2010). *Türkiye'deki organizasyonların bilgi güvenliği olgunluk seviyelerinin belirlenmesi & ISO/IEC 27001:2005 standardına uyumluluklarının değerlendirilmesi*, İstanbul Teknik Üniversitesi Bilim ve Teknoloji Enstitüsü, İstanbul

Baykara, M., Daş R., & Karadoğan İ. (2013). *Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi*. In 1st International Symposium on Digital Forensics and Security (ISDFS'13). Elazığ.

Canbek, G. & Sağıroğlu Ş. (2006). *Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme*. Politeknik Dergisi. 9(3), 165-174.

Colwill, C. (2009). *Human factors in information security: The insider threat – Who can you trust these days?* Information Security Technical Report. 14(4), 186-196.

Çek, E. (2017). *Kurumsal Bilgi Güvenliği Yönetişimi & Bilgi Güvenliği İçin İnsan Faktörünün Önemi*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul

Çetinkaya, M. (2008). *Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması*. Akademik Bilişim, 511-516.

Demirtaş, H. (2013). *Bilgi Güvenliği Yönetiminin Gerekleri & Başarı Dayanakları: Bir Uygulama Örneği*, Yüksek Lisans Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya

Ganbat, O. (2013). *Bilgi güvenliği yönetim sistemi ISO/IEC 27001 & bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması*, Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir

Gaşpar, M.L. & Popescu, S.G. (2018). *Integratıon of the Gdpr Requırements into The Requırements Of the Sr En ISO/IEC 27001:2018 Standard*, Integratıon Securıty Management System in A Software Development Company.

Gencer, K. (2015). ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon

Gikas, C. (2010). *A General Comparison of FISMA, HIPAA, ISO 27000 and PCI- DSS Standards*. Information Security Journal: A Global Perspective. 19(3), 132-141.

Güldüren, C. (2015). *Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi*, Doktora Tezi Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara

Gülmüş, M. (2010). *Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği*,

Yüksek Lisans Tezi Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul

Gürcan, İ.A. (2014). *Finans sektörü için bilgi güvenliği yönetim gereksinimlerinin ISO 27001-tabanlı incelenmesi,* Bahçeşehir Üniversitesi İstanbul

Haklı, T. (2012). *Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi*, Yüksek Lisans Tezi Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, Isparta

Humphreys, E. (2018). *The Future Landscape of ISMS Standards. Datenschutz und Datensicherheit* - DuD. 42(7), 421-423.

Hilton, B.C. (2001). *Information warfare: An evolving perspective,* Baylor University Master of Science in Information Systems, Texas, USA

ISO (2019). International Organization for Standardization. https://www.iso.org/standard/54534.html

ISO/IEC (2017). ISO/IEC:27003 Information Security Management Systems - Guidance. https://www.iso.org/standard/63417.html

ISO/IEC (2016). ISO/IEC:27004 Monitoring, Measurement, Analysis and Evaluation. https://www.iso.org/standard/64120.html

ISO/IEC (2015). ISO/IEC:27006 Requirements for Organizations Providing Audit and Certification of Information Security Management Systems. https://www.iso.org/standard/77722.html

ISO/IEC (2017). ISO/IEC:27007 Guidelines for Information Security Management Systems Audit. https://www.iso.org/standard/77802.html

ISO/IEC (2018). ISO 31000 Risk Management.

https://www.iso.org/standard/65694.html

ISO/IEC (2013). ISO/IEC:27001 Information Security Management System. https://www.iso.org/standard/54534.html.

Dilek, C. (2015). Kuruluşun Bağlamı Nasıl Tanımlanır? http://5s.com.tr/iso-9001-2015de-kurulusun-baglami/.

Başaranoğlu, İ.E. (2016). Information Security Elements. https://www.siberportal.org/blue-team/securing-information/concepts-of-information-security/. Son Erişim Tarihi: 04.02.2019

UEKAE (2008). BGYS Kapsamı Belirleme Kılavuzu.

https://docplayer.biz.tr/101255-Bgys-kapsami-belirleme-kilavuzu.html. Son Erişim Tarihi:

TÜRKAK (2019). Turkey Accreditation Agency.

http://www.turkak.org.tr/.

Kıraç, İ.S. (2015). Information Technology Audit. http://www.btdenetim.net/iso-27001-sertifika-ve-akreditasyon/.

ISO (2017). International Organization for Standardization 2017 Statistic Report. https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse

UHDB, (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. http://www.edevlet.gov.tr/wp-content/uploads/2016/07/2016-2019-Ulusal-e-Devlet-Stratejisi-ve-Eylem-Plani.pdf

UDHB (2017). KamuNet Ağına Bağlanma & KamuNet Ağının Denetimine İlişkin Usul & Esaslar Hakkında Tebliğ. http://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm.

TDK, (2020). Güncel Türkçe Sözlük. http://www.tdk.org.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c077623a1d893.11548437

Bours, D. (2015). The Answer is 42. On Data, Information and Knowledge. URL: https://www.climate-eval.org/blog/answer-42-data-information-and- knowledge.

Governence, I. (2019). Implementing an ISMS. URL: https://www.itgovernance.co.uk/blog/how-to-implement-an-isms. Last Access Date: 10.03.2020

ISACA (2019). ISACA http://www.isaca.org/COBIT/Pages/default.aspx.

Kılıç, M.Ç. & Gökçöl O. (2010). *Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi.* In 3. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu. Ankara.

Kemmler, B. (2018). *An Integrated Service and Security Management System*. 6(1), 1 -12.

King, K.E. (2017). *Examine the relationship between information technology governance, control objectives for information and related technologies, ISO 27001/27002, and risk management,* Ph.D., Minneapolis, USA

Lainhart, J.W. (2000). *COBIT™: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities*. Journal of Information Systems. 14(s-1), 21-25.

Matúš, H. & Martın J. (2009). *Implementatıon of Securıty Controls Accordıng to ISO/IEC 27002 in a Small Organisation*.

Mete, H. (2010). *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin bilgi işlem merkezlerinde uygulanması,* Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya

Nurul, A. (2018). *Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT*. IndoDev Niaga Internet. In International Conference on Computation in Science and Engineering. Jakarta, Indonesia.

Nurbojatmiko, (2016). *Assessment of ISMS based on standard ISO/IEC 27001:2013* at DISKOMINFO Depok City. In 2016 4th International Conference on Cyber and IT Service Management. Bandung, Indonesia.

Shameli-Sendi, A., Aghababaei-Barzegar R., & Cheriet M. (2016). *Taxonomy of information security risk assessment (ISRA)*. Computers & Security. 57, 14-30.

Shoraka, B. (2011*). An Empirical Investigation of the Economic Value of Information Security Management System Standards*, Ph.D., Nova Southeastern University Graduate School of Computer and Information Sciences, Florida, USA

Raflesia, S.P., Surendro K., & Passarella R. (2017). *The user engagement impact along information technology of infrastructure library (ITIL) adoption.* In 2017 International Conference on Electrical Engineering and Computer Science (ICECOS). Palembang, Indonesia.

Rhodes-Ousley, M. (2013). *Information Security, Complete Reference*. (Issue), McGraw-Hill Education: San Francisco.

von Solms, R. (1998). *Information security management (3): The Code of Practice for Information Security Management (BS 7799)*. Information Management & Computer Security. 6(5), 224-225.

Vural, Y. (2007). *Kurumsal Bilgi Güvenliği & Sızma (Penetrasyon) Testleri*, Yüksek Lisans Tezi Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara

APPENDIX

Table of Survey

A. Examination of Information Security Management System from the Perspective of Executive Management

Part I. Personal Information

Below are questions to determine your personal characteristics. For each question posed to you, Mark (X) against the most appropriate option for your situation.

1. Gender?

() Female () Male

2. Your age?

( ) Age 20 and under

( ) Ages 21 to 30

( ) Ages 31 to 40

( ) Ages 41 to 50

( ) Ages 51 to 60

( ) Over 60 years of age

3. Your Level of Education?

() High School () Associate Degree ( ) Bachelor's degree ()

() Ph. D. () Other

4. Occupation?

……....

Survey forms Part 2. About ISO27001 ISMS		**Strongly Disagree**	**Disagree**	**Indecisive**	**Agree**	**Strongly Agree**
1.	ISO/IEC 27001 standard is necessary for our corporation.					
2.	ISO/IEC 27001 Certification gives national and international respect.					
3.	ISO/IEC 27001 provides an easy way to reach our corporate objectives in the field of Information Security.					
4.	ISO/IEC 27001's information security policies are useful in implementing corporation processes.					
5.	ISO/IEC 27001 contributes positively to the information security awareness of corporate managers.					
6.	Management support is important for the Information Security Management System to be sustainable.					
7.	Duties of management are applicable in the ISO / IEC 27001 Information Security Management System.					
8.	Implementation of the ISO/IEC 27001 standard brings additional workload.					
9.	Management should privilege within IT systems.					
10.	ISO/IEC 27001 provides complete internal security as well as external security.					
11.	System would protect us in case of a critical security problem that will occur in general or locally under ISO/IEC 27001.					
12.	Information Security Management Systems cannot manage efficiently without ISO/IEC 27001 certification.					

B. Information Security Management System, Information Security Management System from the Perspective of Staff

Part I. Personal Information

Below are questions to determine your personal characteristics. For each question posed to you, Mark (X) against the most appropriate option for your situation.

1. Gender?

() Female () Male

2. Your age?

( ) Age 20 and under

( ) Ages 21 to 30

( ) Ages 31 to 40

( ) Ages 41 to 50

( ) Ages 51 to 60

( ) Over 60 years of age

3. Your Level of Education?

() High School () Associate Degree ( ) Bachelor's degree ()

() Ph. D. () Other

4. Occupation?

…….....

Survey forms Part 2. ISO27001 Management Process		**Strongly Disagree**	**Disagree**	**Indecisive**	**Agree**	**Strongly Agree**
1.	ISO/IEC 27001 standard is necessary for our corporation that consulting services should provided in order to manage the Information Security Management System processes					
2.	ISO/IEC 27001 standard is necessary for our corporation that the staff of our corporation is sufficient to manage the Information Security Management System processes.					
3.	ISO/IEC 27001 standard is necessary for our corporation the staff should trained to manage information security management system processes.					
4.	ISO/IEC 27001 standard is necessary for our corporation the staff that will established should consist of IT staff.					
5.	Number of our organization's information security staffs are sufficient to manage ISO27001 processes in a healthy way.					
6.	Healthy work could carry out with the staff of the corporation during the management of ISO / IEC 27001 processes.					
7.	During the corporate risk studies, enough support could obtain from the corporation staff.					
8.	ISO/IEC 27001 processes could implement in a healthy way in our corporation.					
9.	ISO/IEC 27001 standard is necessary for corporate information security.					
10.	ISO/IEC 27001 provides complete internal security as well as external security.					
11.	The measures taken under ISO/IEC 27001 would protect us against critical information security problems from within or outside the organization.					
12.	It is difficult for people to abandon their habits during the transition to ISO/IEC 27001 system.					
13.	The workload on IT staff has decreased after the transition to ISO / IEC 27001 system.					

14.	The policies and procedures set out in the framework of ISO/IEC 27001 open up the clogged corporation's processes.					

C. Examination of Information Security Management System in Terms of Technical Personnel and Competencies

Part I. Personal Information

Below are questions to determine your personal characteristics. For each question posed to you, Mark (X) against the most appropriate option for your situation.

1. Gender?

() Female () Male

2. Your age?

( ) Age 20 and under

( ) Ages 21 to 30

( ) Ages 31 to 40

( ) Ages 41 to 50

( ) Ages 51 to 60

( ) Over 60 years of age

3. Your Level of Education?

() High School () Associate Degree ( ) Bachelor's degree ()

() Ph. D. () Other

4. Occupation?

…….....

Survey forms Part 2. General considerations on ISO27001		**Strongly Disagree**	**Disagree**	**Indecisive**	**Agree**	**Strongly Agree**
1.	Number of Tech Staff is sufficient in order to conduct the Information Security Management System processes in a healthy way.					
2.	The ISO/IEC 27001 standard is applicable in enterprise IT processes.					
3.	We should get training/trainings related to ISO/IEC 27001.					
4.	IT systems have become easier to manage that with the introduction of ISO/IEC 27001 standard.					
5.	ISO/IEC 27001 benefits me from being able to carry out the processes related to my task effectively and in a timely manner.					
6.	Due to the measures taken under ISO/IEC 27001, there has been a reduction in information security					
7.	The ISO/IEC 27001 standard contributes positively to the security of developed enterprise applications.					
8.	Incidents of information security breaches have reached the point where they could control with ISO / IEC 27001.					
9.	It is useful to implement regulatory and preventive activities on the faults identified in Information Systems.					
10.	There will be less problems on a system that has taken more security measures within the scope of ISO / IEC 27001.					
11.	If all processes of the ISO/IEC 27001 standards operated in the best way possible risks can identified in advance.					

D. Examination of Information Security Management System in Terms of Staff And Competencies

Part I. Personal Information

Below are questions to determine your personal characteristics. For each question posed to you, Mark (X) against the most appropriate option for your situation.

1. Gender?

() Female () Male

2. Your age?

( ) Age 20 and under

( ) Ages 21 to 30

( ) Ages 31 to 40

( ) Ages 41 to 50

( ) Ages 51 to 60

( ) Over 60 years of age

3. Your Level of Education?

() High School () Associate Degree ( ) Bachelor's degree ()

() Ph. D. () Other

4. Occupation?

…….....

Survey forms Part 2. General considerations on ISO27001		**Strongly Disagree**	**Disagree**	**Indecisive**	**Agree**	**Strongly Agree**
1.	Information training about ISO/IEC 27001 is sufficient.					
2.	Content of the information trainings given about ISO/IEC 27001 is sufficient.					
3.	Materials and samples given during the information trainings about ISO/IEC 27001 are adequate and up-to-date.					
4.	Information security training I have received is useful.					
5.	Information given in the scope of the trainings is applicable in terms of corporation's processes.					
6.	Content should be full rather than the duration of the trainings given within the scope of the					
7.	The trainings completed enough only through slides.					
8.	Company that provided the training also conveyed the experiences it obtained from other customers.					
9.	Measures taken in the context of Information Security have severely restricted user privileges.					
10.	Information Security Management Systems carried out in our corporation well managed.					