INFORMATION SECURITY MANAGEMENT SYSTEM AND INFORMATION SECURITY RISK MANAGEMENT METHODOLOGY DEVELOPMENT

by

Ayfer Ekiz

Submitted to Graduate School of Natural and Applied Sciences
in Partial Fulfillment of the Requirements
for the Degree of Master of Science in
Systems Engineering

Yeditepe University
2019

INFORMATION SECURITY MANAGEMENT SYSTEM AND INFORMATION SECURITY RISK MANAGEMENT METHODOLOGY DEVELOPMENT

APPROVED BY:

Assist. Prof. Dr. Zeynep Ocak ....Zeynep Ocak..........
(Thesis Supervisor)
(Yeditepe University)

Assoc. Prof. Dr. Dilek Tüzün Aksu ....
(Yeditepe University)

Assist. Prof. Dr. Melis Almula Karadayı ....
(Medipol University)

DATE OF APPROVAL: ..../..../2019

ACKNOWLEDGEMENTS

I first thank my dear supervisor Assist. Prof. Dr. Zeynep Ocak, for her support and guidance.

I also want to thank my colleague Erkan Kırat for his suggestions and contributions.

Finally, I sincerely thank my deceased father, whose love I always felt in my heart.

ABSTRACT

INFORMATION SECURITY MANAGEMENT SYSTEM AND INFORMATION SECURITY RISK MANAGEMENT METHODOLOGY DEVELOPMENT

Information security is the protection of information from threats in order to ensure business continuity by reducing business risks, and maximizing return on investments and business opportunities. In strategic terms, the confidentiality, integrity and availability of crucial information must be provided via an effective information security management system to ensure business continuity.

In today’s world, information is exposed to a growing number of threats. Thus, ensuring the information security is vital for today’s interconnected business environment. Information security policies are the basis for a reliable information security system and are critical to protect the organisation’s Information System (IS) resources and data.

ISO 27001:2005 provides a widely-accepted information security management guideline for establishing, implementing, operating, monitoring, maintaining and improving an information security management system (ISMS). Although it is suitable for all kinds of organizations there is a lack of a comprehensive framework, supporting process model, and methodology that can enable an enterprise to implement and effectively manage information security. Thus, the purpose of this study is to examine a pharmaceutical firm’s information security management system, and to develop an appropriate framework and methodology to ensure integration of information security management with other enterprise business processes.

ÖZET

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE BİLGİ GÜVENLİĞİ RİSK YÖNETİMİ METODOLOJİSİ GELİŞTİRME

Bilgi güvenliği, iş risklerini azaltarak, yatırım geri dönüşlerini ve iş fırsatlarından faydalanmayı maksimize ederek, iş sürekliliğini sağlamak için bilgilerin tehditlerden korunması anlamına gelmektedir. Stratejik açıdan, iş sürekliliğini sağlamak için çok önemli olan bilgilerin gizliliği, bütünlüğü ve erişilebilirliği etkin bir bilgi güvenliği yönetim sistemi ile temin edilmelidir.

Günümüz dünyasında, bilgiler gittikçe artan sayıda tehdide maruz kalmaktadır. Bu nedenle, bilgi güvenliğinin temin edilmesi günümüzün birbirine bağlı iş ortamları için hayati öneme sahiptir. Bilgi güvenliği politikaları, güvenilir bir bilgi güvenliği sisteminin temelidir ve kuruluşun bilgi sistemi (BS) kaynaklarını ve verilerini korumak açısından kritik bir öneme sahiptir.

ISO 27001: 2005, bilgi güvenliği yönetim sistemi (BGYS) oluşturmak, uygulamak, işletmek, izlemek, sürdürmek ve geliştirmek için yaygın olarak kabul edilen bir bilgi güvenliği yönetim kılavuzu niteliği taşır. Bu standart her türlü kuruluşun kullanımı için uygun olmasına rağmen, işletmelerin bilgi güvenliğini uygulayabilmesini ve etkin şekilde yönetmesini sağlayacak kapsamlı bir çerçeve, destekleyici süreç modeli ve metodoloji sunmamaktadır.

Dolayısıyla, bu çalışmanın amacı bir ilaç firmasının bilgi güvenliği yönetim sistemini incelemek ve bilgi güvenliği yönetiminin diğer kurumsal iş süreçleri ile entegrasyonunu sağlamak üzere uygun bir çerçeve ve metodoloji geliştirmektir.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS/ABBREVIATIONS

ALE	Annualized loss expectation
BGYS	Bilgi güvenliği yönetim sistemi
BS	Bilgi sistemi
BS	British Standard
BSI	British Standards Institute
DTI	Department of Trade and Industry
FDA	Food and Drug Administration
GSM	Global system for mobile
IEC	International Electrotechnical Commission
IS	Information system
ISMS	Information security management system
ISO	International Organization for Standardization
IT	Information technology
KPI	Key performance indicators
NDA	Non-disclosure agreements
PDCA	Plan, do, check, act
R& D	Research and development
SOA	Statement of applicability

1. INTRODUCTION

As a consequence of the developing spread of correspondence media and the exponential increment in the rate of transmission of data and electronic storage, the requirement for information security has reached extreme levels for both personal and institutional use. Some significant causes behind this requirement can be specified as the increase in electronic applications in organizations, sharing information over network systems, having the option to obtain information from many resources, rapidly rising threat of data loss, and above all increase in financial and reputational loss [1]. Posthumus and Solms [2] claimed that information is the most valuable assets of many organizations in today's stiff competition environment and for this reason it should be protected, secured and managed properly. Whitman and Mattord [3] added disclosure or abuse of information causes loss of time, manpower, money and/or business opportunities.

Information security is the protection of information from threats in order to ensure business continuity by reducing business risks, and maximizing return on investments and business opportunities. In modern times, information is exposed to a growing number of threats. So, ensuring the information security is vital for today's interconnected business environment. Information Security Policies are the basis for a reliable information security scheme and are critical to protect the organisation's Information System (IS) resources and data. Information system security generally consists in ensuring that an organisation's material and software resources are used only for their intended purposes [4].

As a result, the security attention in information systems has grown in recent years due to increasing number of critical corporate information assets, their rapid dissemination and exposure to possible attacks. In strategic terms, it must be emphasised the confidentiality, integrity and availability of information, often crucial to ensure business continuity.

ISO 27001:2005 standard [5] provides a widely-accepted information security management framework for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS). It is also suitable for all kinds of organizations regardless of country and sector. Almost all organizations follow ISO 27001:2005 standard [5] during their ISMS related implementations.

1.1. HISTORY OF THE ISO/IEC 27001:2005 STANDARD

The information security management standards of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), trace their roots to British information security standards of 1990s. Over the past decade, ISO/IEC information security standards have been gradually revised through extensive public consultations and inputs from various industries, and are now widely adopted across the world. The management of information security from a people, processes, and systems point of view is the core objective behind the approach taken by ISO/IEC information security management standards [6].

In the early 1990s, the Department of Trade and Industry (DTI) in the United Kingdom set up an industry group to produce a code of good information security practice. In 1992, DTI published a document titled, “A Code of Practice for Information Security Management”. In 1995, this document was amended and re-published by the British Standards Institute (BSI) as a guidance document, and later that year, as the BS 7799:1995 standard. Following an extensive revision and public consultation period that began in November 1997, the first revision of the standard was published in April 1999.

The original code of practice was significantly revised and retained as BS 7799:1999 Part 1. The title of the standard was “Code of Practice for Information Security Management”. The BS 7799:1999 Part 1, commonly referred to as BS 7799-1, was proposed as an ISO standard in October 1999, and published with minor amendments as ISO/IEC 17799:2000 in December 2000. As a result of the regular ISO standards update cycle, the ISO/IEC 17799:2000 was republished in 2005 as ISO/IEC 17799:2005, and renamed to ISO/IEC 27002:2005 in 2007. The title of the ISO/IEC 27002 standard is “Information technology – Security techniques – Code of practice for information security management”. The standard establishes guidelines for initiating, implementing, maintaining, and improving information security management in an organization. It provides general guidance on the commonly accepted goals of information security management [7].

The BS 7799 Part 2 standard, commonly referred to as BS 7799-2, was introduced in April 1999 and extensively revised in September 2002. The standard was titled, “Specification for an Information Security Management System". It was intended to be used as the means to measure and monitor BS 7799-1, and to provide a benchmark for third-party certification. It detailed the requirements specifications for an information security management system. In 2005, BS 7799-2 became an ISO standard and was published as ISO/IEC 27001:2005 (ISO ISMS). The standard specifies requirements for the implementation of security controls customized to the needs of individual organizations [8].

The ISO ISMS standard consists of 133 security controls that are organized into the following 11 security domains:

- Information security policy.
- Information security organization.
- Asset management.
- Human resources security.
- Physical and environmental security.
- Communications and operations management.
- Access control.
- Systems development and maintenance.
- Information security incident management.
- Business continuity management.
- Compliance.

All of the 133 controls in these domains may not be applicable for every organization. So, the selection of adequate security controls in accordance with the business line of each organization is required. All of these controls are applicable to our study and the controls performed in the case is documented under the title of "Statement of Applicability (SOA)". An organization that meets the requirements of the standard by providing the applicable controls is granted the ISO 27001 certification from an accredited certification body. According to Thomas and Botha [9], the ISO ISMS certification has earned a reputation as the internationally acceptable "de facto" standard for information security management.

According to Rowlingson and Winsborrow [10], the ISO ISMS certification is widely perceived as a benchmark for excellence in information security.

1.2. BACKGROUND OF THE STUDY

Organizations gain big competitive advantages by getting ISO 27001 certificates. International Standards Organization performs annual survey indicating the worlwide statistics of management systems certifications. According to the ISO survey report of 2015, there are 27536 valid ISO 27001 certificated companies all over the world as of 31 December 2015. The figure for 2014 was 23005. So, there is a 30 % increase over the previous year. This growth demonstrates that the importance of Information Security is increasing significantly.

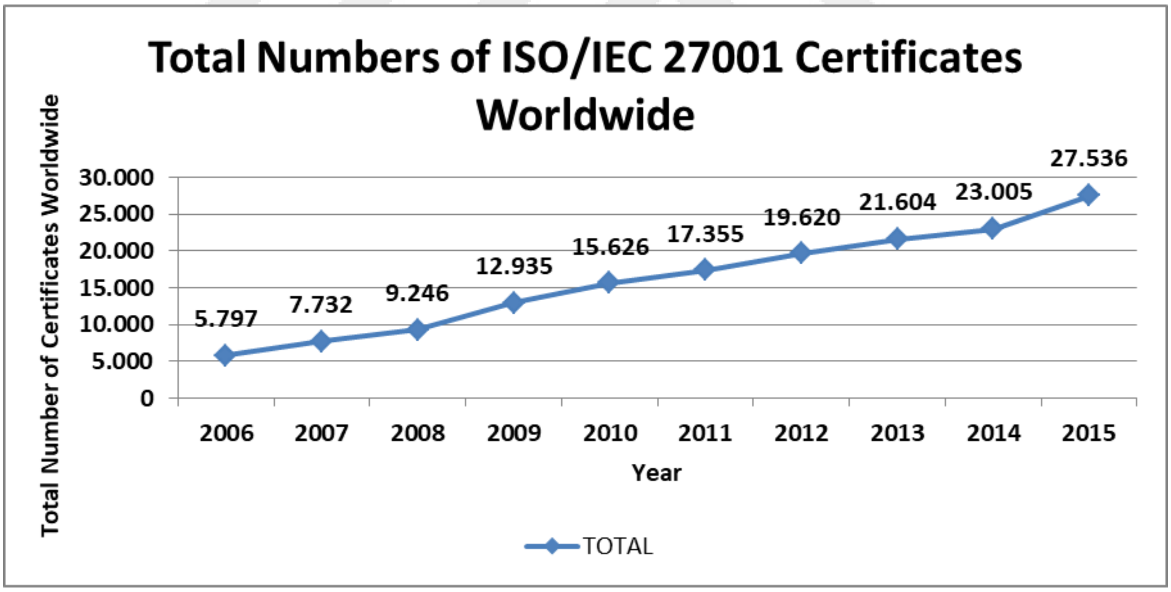


Figure 1.1. Total numbers of ISO/IEC 27001 certificates worldwide. (The ISO survey report of 2015)

As it can be seen in the Figure 1.1, over the past decade number of certificated companies increased dramatically.

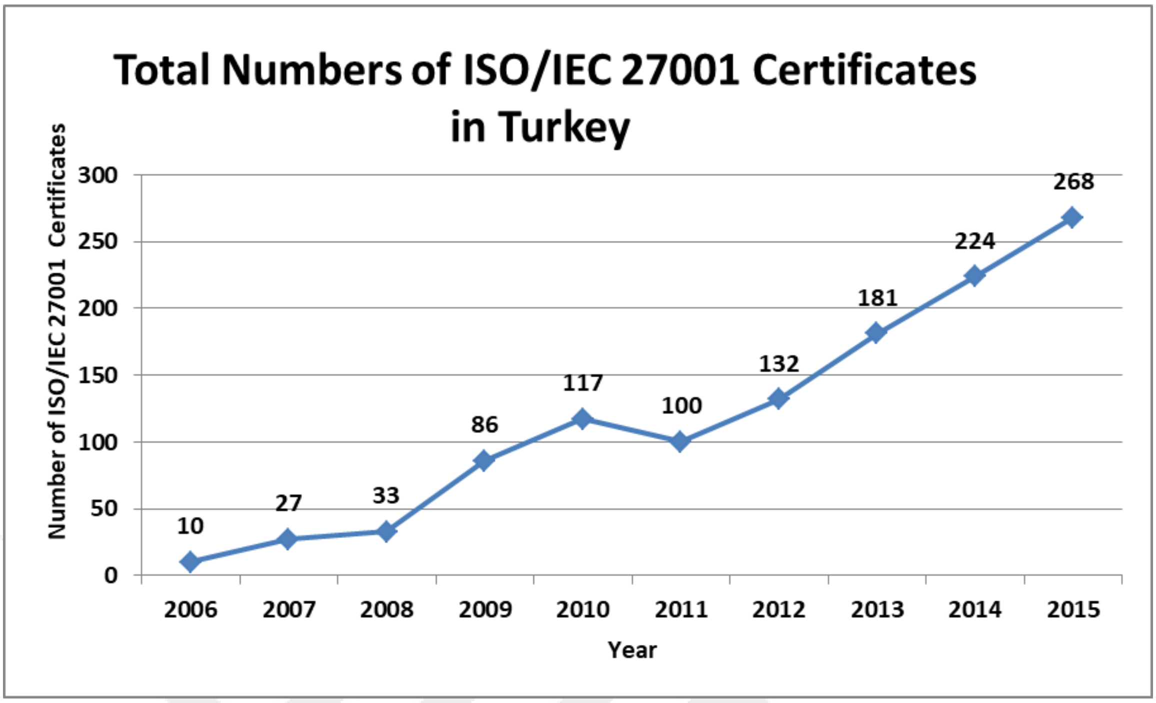


Figure 1.2. Total numbers of ISO/IEC 27001 certificates in Turkey. (The ISO survey report of 2015)

The Figure 1.2 shows that the trend in Turkey is similar to the trend in the world.

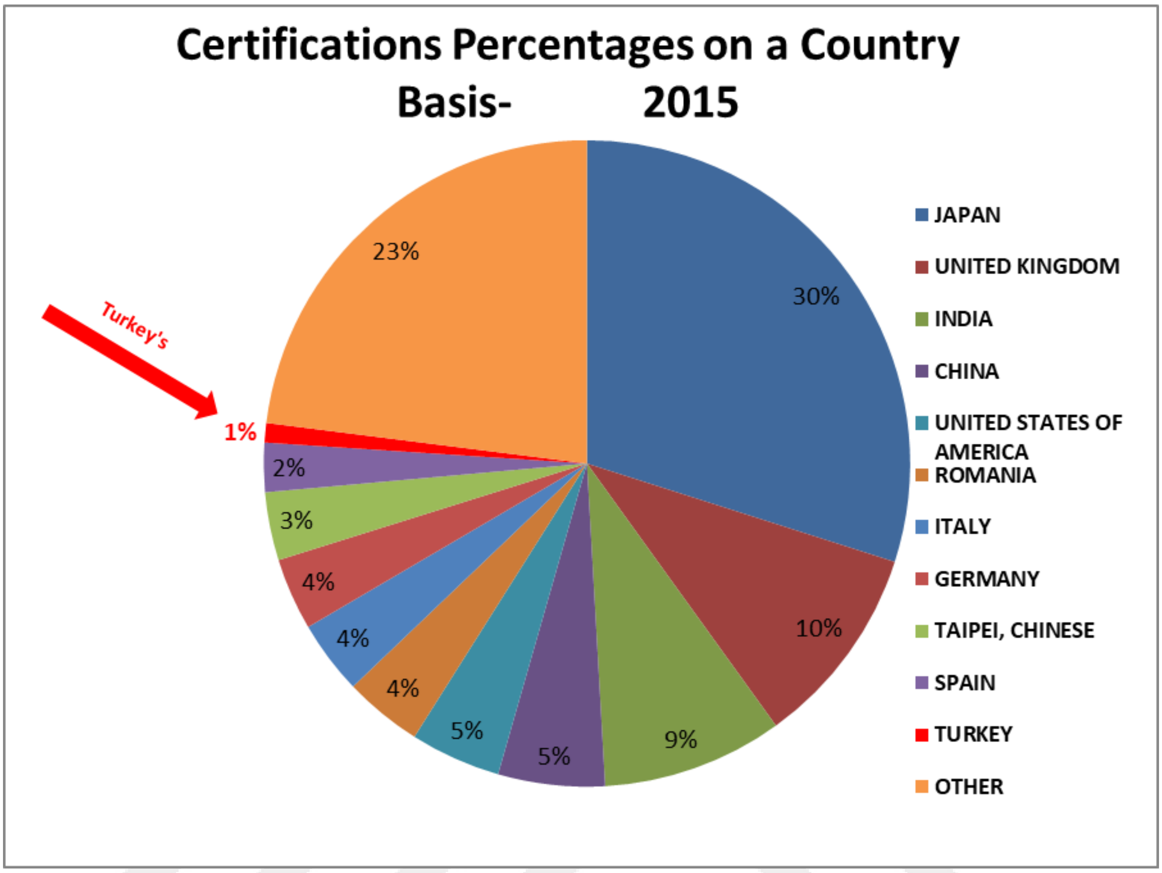


Figure 1.3. Percentages on a country basis-2015. (The ISO survey report of 2015)

As it can be seen in the Figure 1.3 Japan has the largest share in the world distribution of ISO/IEC 27001 certificates in 2015. Turkey ranked 17th in this distribution with a one percent share.

The most important determining factor for this ranking is the legal obligations and regulations in countries. For example, in Japan as a cyber security strategy, being certificated is a legal obligation for all kinds of organizations. On the other hand, in Turkey, ISO 27001 certification is mandatory only for organizations providing communication services.

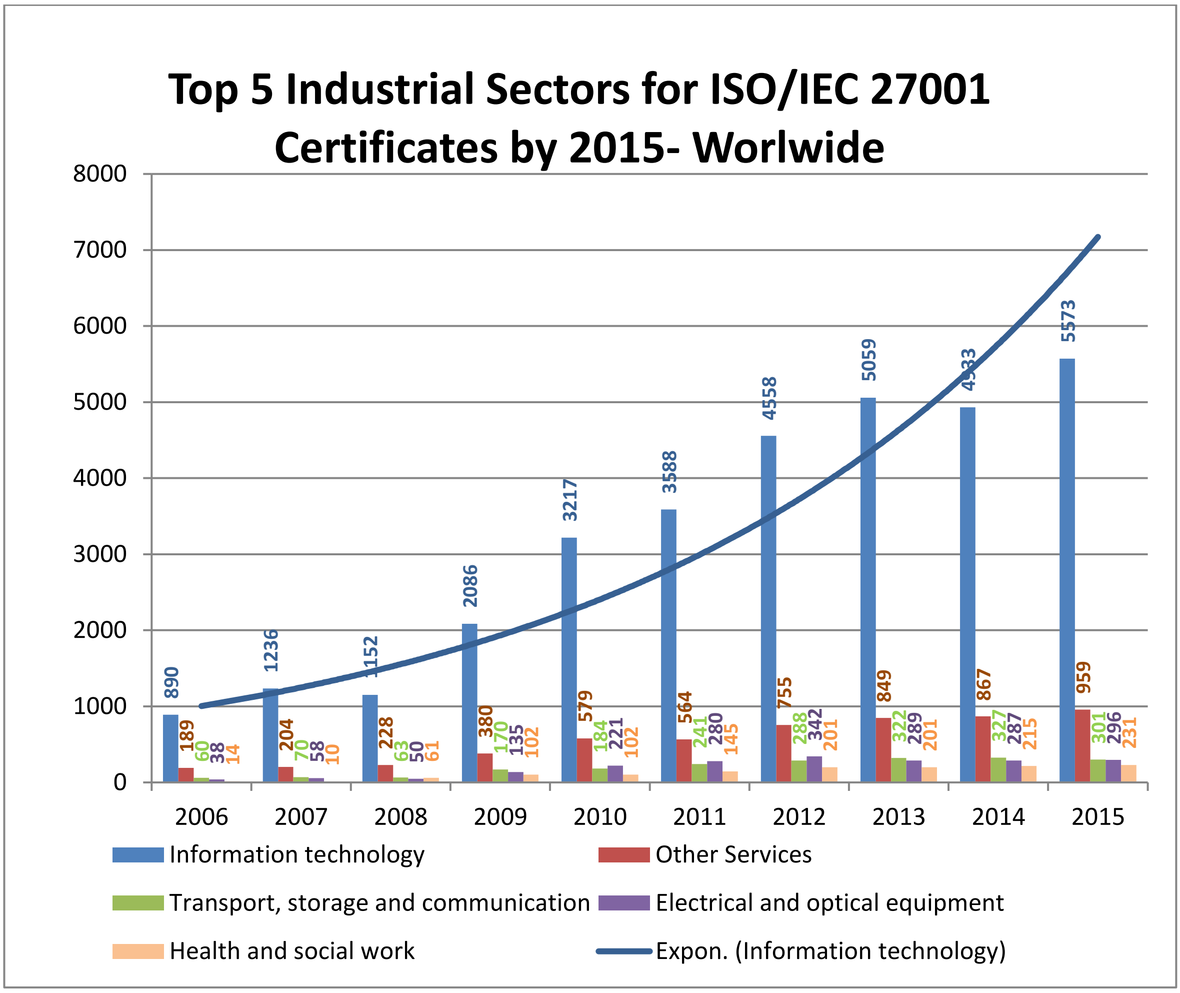


Figure 1.4. Top five industrial sectors for ISO/IEC 27001 certificates by 2015- worlwide. (The ISO survey report of 2015)

The Figure 1.4 shows the top 5 certificated industrial sectors among 39 different industrial sector. As it is seen in this figure number of certification shew a sharp increase from 2006 to 2015 in each industry. As it can be seen in the Figure 1.4, from 2006 to 2015, the highest rate of certication increase was in the health industry (which includes pharmaceutical industry) approximately 16 times.

In our research we focused on pharmaceutical industry which shows the biggest proportional increase.

As Deloitte Tohmatsu Consulting Co., Ltd. [11] claimed, the most valuable information of a pharmaceutical company is the formula of its new drugs. Internal threats like theft of trade secrets are as important as external threats like hackers. In the same study, it is stated that pharmaceutical, biotechnology and healthcare sector's estimated lost due to information theft is ₤1.8 billion for UK and $500 billion for US in 2011. Total cost for global pharmaceutial market is estimated as $1.1 trillion for the same year.

Deloitte Tohmatsu Consulting Co., Ltd [11] stated that major US pharmaceutical companies including medical device-maker, Boston Scientific, Abbott Laboratories, and Wyeth, the drug maker acquired by Pfizer Inc. were attacked by a sophisticated Chinese hacking group. The same group also successfully hacked the Food & Drug Administration's computer center in Maryland and exposed sensitive data (including formulas and trial data) for almost all drugs sold in US.

As a result, companies decided to invest in Information Security measures like breach alarm systems which alert the security team in case of any intrusion and unauthorized access attempt.

The company in our study is also in pharmaceutical sector. The company fights against counterfeit drugs and aims to protect its sensitive drug development data, formulas. In accordance with this purpose we first developed a methodological framework for information security management system, based on ISO 27001 requirements. Next we prepared process maps which guide companies during implementation of information security management activities. Finally, we follow the framework and process maps for implementation of information security management processes like identification of security objectives, risk management, management of information security breaches etc.

2. PURPOSE OF THE RESEARCH

The purpose of this study is to examine corporate information security management system, and to develop an appropriate framework and methodology, which could enable integration of information security management with other enterprise business processes.

Specifically, we can summarize the main objectives of this study as follows:

- To develop an appropriate methodological framework that is compatible with the ISO 27001:2005 standard.
- To develop process maps for each step of the methodological framework to guide users during their implementation.
- To implement this framework to a pharmaceutical company.

2.1. PROBLEM STATEMENT

There is a lack of a comprehensive framework, supporting process model, and methodology that can enable an enterprise to implement and effectively manage information security. ISO 27001 standard provides a baseline for ISMS implementations and tells what to do for ensuring information security, but it does not tell how to carry out ISMS processes. For example, a risk assessment is used to identify the controls required by the organization. However, ISO 27001 does not define the risk assessment method to be used, it only ask you to provide the requirements included in the standard. Thus there is a lack of guidance for organizations that are willing to implement ISO 27001.

What makes this study significant is that by providing a framework, executives will be able to better understand and implement the information security management system within their organizations. Additionally, the process maps developed will break down the complexity of ISMS processes, thus improve the understanding of process flows. This will also enable companies to define steps for improvement of ISMS processes.

3. LITERATURE REVIEW

We reviewed the literature in accordance with the developed methodological framework including general overview of ISMS and ISO 27001 standard and risk management strategies.

Recent Information Systems (IS) security studies have emphasized several important themes such as IS security effectiveness, security planning and risk management, the economics of IS security and evaluation of IS security investments, designing and maintaining IS security systems. Brenner [12] viewed the ISO 27001 (ISMS) standard as an overall program that combines risk management, security management, governance and compliance, and Hazari [13] observed that an information security plan that includes technology, personnel, and policies is the best approach to developing an enterprise information security strategy.

Organizations adopt information security standards to gain competitive advantage by ensuring their customers and business partners that recognized processes are in place to deal with information security threats [9].

Security professionals claim that the ISO ISMS standard is a suitable model for addressing information security management issues in the modern organization, and its controls define an industry baseline of good security practices.

As ISO ISMS standard offers a holistic approach and provides a competitive advantage by means of its globally accepted reputation, organizations ground on this standard during formation of their ISMS framework. We also adapt our study to this standard for the same reasons.

ISMS should be effectively implemented in order to be useful for the organization. ISMS is not an application to be completed at once. It should be seen as a sustainable process for continuous improvement. Hence, it must be a part of business and operational culture. Well-choosen information security controls in this system will not cause cost, contrarily it will contribute to the success of the organization as long as it is compatible with company goals [14].

As stated by Johnston et al. [15] preparing comprehensive company goals is the essential principle and first step of Information Security Management System (ISMS). Siponen et al.’s [16] expression in the same study “The determination of common objectives is important for both establishing the starting point for effective information security programs and for establishing evaluation criteria for diagnostic purposes” supports this idea.

Information security objectives and organizational policies aligned with these objectives provide proper protection of information assets and awareness of employees on ISMS. They also ensure that all business processes are carried out in line with the organization’s information security rules.

Violation and misuse of information systems by employees have been identified in the extant literature as the most important issue for an organization in terms of information security. Prevention against this threat can be provided by creating information security awareness and stating the responsibilities on employee basis. “Employees who use the information and technology resources of their organizations, assume certain roles in and are responsible for safeguarding (protecting) those resources, so we are interested in what factors drive an employee to perform those roles and meet their responsibilities. We define information security policy as a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations.” [17].

Safa et al. [18] also point out that compliance with organizational information security policies shapes employee’s attitude and minimizes the security risks. According to the same study, in spite of some technologic security solutions such as anti-virus programs, firewall, intrusion detection systems, information security is not guaranteed. Most of the cyber attacks are organized by exploiting users’ misbehavior such as opening unknown e-mails, using simple passwords or sharing their username and password with colleagues. Consequently, all these examples demonstrate that employees’ awareness and precision play a vital role in an organization’s information security management.

Allocating responsibilities and giving chance to contribute to information security activities influence employees’ motivation by means of job satisfaction [18]. Consequently, employees who are more committed to the organization are less likely to deviate from the security policies.

Lee and Lee [19] proposed a conceptual research model based on deterrence theory and several social theories to explain the influence of organizational factors, information security policy and information awareness programs on preventing computer abuse. Straub and Nance [20] also investigated how to discover computer abuse and discipline perpetrators, suggesting that organizations should punish serious violations to the full extent permitted by law because such punishment would deter other such behavior. The information security rules must be determined and declared to the personnel in order to operate the penalty system in case of any information security violation.

Mostly, organizations specify information security rules in their information assets classification policy. Chen et al. [21] pointed out that insufficient preservation of information assets causes many information systems incidents. He continued that, asset classification policies enable organizations to determine exact corresponding information security controls for each asset class. Park et al. [22] compiled a check list based on ISO 27001 standard and investigated the Information Security Management Systems of five big hospitals. This study shows that asset management and information classifications, were the most sensitive part of the ISMS, and concluded that the most frequently encountered problems were lack or weak identification of asset classification manual, missing assets in the inventory list and uncertainty in assets ownership and related responsibilities. Bergström and Åhlfeldt [23] noted that various studies highlight the fact that altough information classification is not a new concept, a lot of companies have difficulties with information assets classification.

Bergström and Åhlfeldt [23] also stated that the impact of the risk is evaulated according to the information classification criteria which indicates information assets' value and criticality. So, they claimed that information classification is the one of the most important input for risk analysis.

Blakley et al. [24] discussed that information security risk analysis is necessary, due to the fact an organization's information is processed through a technology and this technology brings lots of risks along. They also indicated that improper disclosure of an information may cause confidentiality compromise, wrongly modified information may cause integrity compromise while a lost or destroyed data may result in availability compromise. Violation of these information security attributes (confidentiality, integrity, availability) on a valuable information asset causes direct or indirect costs.

Blakley et al. [24] also specified that, risk analysis is known as the fundamental discipline for the management of information security. There are various risk analysis methodologies some of which are included in formal information security standards. Most of these standards assess the risk calculation parameters like probability and impact of losses in terms of qualitative statements (Low/Medium/High). But some organizations prefer to assess risks quantitatively. They stated that generally accepted method measuring the cost of risk quantitatively is “Annualized Loss Expectation (ALE)”. In the given example, a chemical company estimates the likelihood of an explosion (threat) as one in a million. Also, the cumulative cost is evaulated in case of this disaster considering both the direct (repair cost, loss of machines etc) and indirect expenses (loss of reputation and competitive advantage etc).

In both quantitative and qualitative methods, each threat on each individual asset is assessed. So, the company has a chance to prioritize its actions based on the annual expected losses or risk level (Low/Medium/High) and allocate its resources properly in order to remove or minimize the risks.

Blakley et al. [24] claimed that quantitative risk assessment methods require to assign specific values for the variables like cost of information security breach, likelihood of security incident occurrence, cost of measures taken. The deficiency of good quality data for predicting likelihood of security incident occurrence, expected cost of losses and cost of measures are the main issue in quantitative methods. It is stated in the same study that accurate risk analysis can be harder for information security due to constantly changing risk factors like asset value. For example, value of an asset may change based on the daily exchange rate. For these reasons, today nearly all of risk assessments are conducted by qualitative method [24]. In our study qualitative risk assessment method was used, too.

Rainer et al. [25] defined the steps of information security risk analysis methodology framework in their study. They used the 4-step methodology (asset identification and analysis, threat identification and analysis, vulnerability identification and analysis, risk analysis). This 4-steps methodology is compatible with the risk analysis process which is defined in the existing ISO 27001 Information Security Standard. This standard is a widely accepted guide and today majority of companies establish their Information Security Management System based on this standard. So it means that, Rainer et al. [25] proved that their methodology is applicable to many industries. This methodology is also best fit to our study.

Amancei [26] stated that after performing risk analysis, risk treatment actions must be taken in order to mitigate the level of risks. He also added that selecting one of the risk treatment method (risk avoidance, risk transfer and risk acceptance) depends on the risk score obtained as a result of risk analysis.

Seale [27] performed a risk analysis study in accordance with ISO 27001 information security standard for Health& Care Professions Council. He categorized the risks as strategic risks, communication risks, corporate governance risk, financial risks, operation risk, quality management risks etc. The total number of risks defined for all all categories was 131. He prepared a risk register and risk treatment plan including projects, actions for each risk in order to eliminate the risks or reduce the risk level. Before execution of the risk treatment plan, the number of low level risks was 31, the number of medium level risks was 55 and the number of high level risks was 45. After implementations of projects or activities stated on the risk treatment plan the risk analysis study was performed again and the number of low level risks rose to 118, number of medium level risks dropped to 13 and the number of high level risks was zeroized. This study supports our methodology in terms of the approach indicating that high level risks must be decreased to medium or low level by implementing a project or taking actions.

Measuring the performance of controls and effectiveness of those projects or actions are also critical in Information Security Management System. Peláez [28] claimed that information security budget is limited, it should be allocated properly. He added that return on investment for the information security controls implemented should be justified. Peláez [28] continued that the result of risk analysis is the main input for selection of the information security controls to be implemented. As a result of risk analysis study, risks can be prioritized in terms of their impact on organizational processes. In this way, corresponding controls are defined accurately and in line with the budget. It is also very important to implement these controls in a cost effective way and objectively. He continued that good quality metrics must be defined to measure the effectiveness of those controls. Also, responsibilities and frequency of control parameters must be defined as well. According to Peláez [28], the process of measuring the performance of controls varies from companies to companies or may not be the same for the processes within the organization. Indicators to ensure the efficiency of the security process in reducing the risks must be determined based on each case. Also, these controls should be performed continuously and efficiency of them should be measured periodically to keep the security system alive and repeatable. For this purpose Peláez [28] used a framework called PDCA (Plan, Do, Check, Act) Cycle which is proposed in ISMS standard to ensure the system continuity.

Peláez [28] performed a study for an electricity distribution company. As uninterrupted delivery of electricity is critical for Information Security especially in terms of availability, he determined risks and KPIs (Key Performance Indicators) which aim at mitigation of the power interruption risks. After matching KPI's and related risks, he determined specific controls to mitigate the likelihood of risk occurrence. He claimed that defining what level of risks can be tolerated is essential to avoid unnecessary expence on performance measurement of the security controls. Concordantly, he used 5-level scale (Catastrophic, Higher, Moderate, Minor and Insignificant) and allocated limited information security budget accurately. He also measured the effectiveness of controls by comparing target (expected) value and actual value. In our study we measured the effectiveness of information security controls with a similar approach in Peláez's [28] study.

Due to the everchanging environment and conditions, the processes mentioned in Peláez's [28] study must be carried out continously in a living organization. To keep up with these changes and to mitigate the risk by giving instant responses to threats, organizations make great effort on management of security events and breaches.

Almost everyday we hear about lots of cyber attacks. These attacks threaten all kinds of business even governments and cause large amount of tangible and intangible costs. Moreover, they might lead to bankruptcy of companies. So, organizations allocate big budgets for information security to ensure their business continuity. Scarfone et al. [29] remarked that new types of information security events/breaches rise rapidly and demonstrated the ever-increasing trend in his study. So, an effective response capability is vital to immediately detecting those threats and minimizing losses. Response methods depend on the nature of the incidents.

According to same study, establishing an incident response capability should include the following actions:

- Creating an incident response policy and plan.
- Developing procedures for performing incident handling and reporting.
- Setting guidelines for communicating with outside parties regarding incidents.
- Selecting a team structure and staffing model.
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies).
- Determining what services the incident response team should provide staffing and training the incident response team.

Management review of ISMS is as important as management of security events and breaches, for sustainability of the system. Regular meetings with the participation of top management are held. ISO 27001 requires that this meeting be held at least once a year for the certification. As it is stated by Kosutic [30] management review of ISMS is must be done in a systematic way by the participation of top management. Crucial decisions, such as increasing the budget for this system, obtaining a new tool, readjusting the resource allocation and restructuring the organizational form etc, are taken in this meetings in order to improve the effectiveness of the system. In our study the frequency of management review meeting is stated as once in the procedure, but in case of any need such as big changes it could be done more frequently.

As seen in the literature ISO 27001 standard is widely accepted and it is a general guide for information security management system, but it does not offers a concrete methodology for implementation of ISMS. Our purpose is to provide a clear methodology in order to make ISO 27001 more understandable and practicable for information security management system implementations. ISO 27001 is also commonly used in pharmaceutical industry. Adulteration in medicine, counterfeiting and theft of know how or intellectual property are the most severe threats for this sector. Due to all these reasons, in this sector ISMS is essential for survival of the company. In our study we will suggest a methodological framework in accordance with ISO 27001 standard and provide process maps to support the pharmaceutical industry in terms of proper implementation of ISMS. We will also provide an application example.

4. METHODOLOGY

The key objectives of the ISO 27001 standard are to identify possible information security vulnerabilities of the organization, to identify threats against information assets, to systematically monitor these threats, to keep risks at an acceptable level and to ensure continuity of the system. Just like every standard, ISO 27001 is a general guide to for the wide range of organization, it only tells what to do, not how to do it and specifies minimum requirements for an effective ISMS. So, every organization should prepare an ISMS framework specific to its field of operation by accepting the standard as the basis.

In this research, we developed a comprehensive Information Security Management System (ISMS) framework by adopting the ISO 27001 standard as a basis. Although the standard provides a good baseline for ISMS implementation as indicated before it does not illustrate how to administer and control the ISMS processes. Thus the comprehensive framework we developed will be helpful in this regard, and will help to enable pharmaceutical companies to implement ISMS effectively. We also developed process maps using business process mapping method to explain in detail how to implement information security management system in a pharmaceutical company.

4.1. BUSINESS PROCESS MAPPING

A business process is a series of activities performed by a group of stakeholders to achieve a spesific goal.

Business Process Mapping refers to the strategic analysis of defining and generating a visual depiction of those business processes of various areas in an organization. A business process map helps to visualize the responsible parties of each process step. Thus, a process map makes it clear who is in charge of each activity of a process and provides better understanding of how your business functions are carried out.

There are various advantages of using business process maps. These are revealing the strengths and weaknesses of processes, identifying areas with inefficiencies. Business process mapping is also an excellent tool for anticipating potential risks caused by threats in the processes.

As, Information Security Management is a risk based system, we prepared and used process maps in order to identify and eliminate the information security risks in our processes.

4.2. IDENTIFICATION OF SECURITY OBJECTIVES

The main purpose of establishing ISMS (Information Security Management System) in a company is to protect the sensitive information assets from all threats coming from inside/outside, intentionally/accidentally in terms of confidentiality, integrity, availability to create a sustainable environment. Identifying security objectives is essential to achieve this purpose.

As a first step of identification of security objectives process ISMS scope is determined considering the environment in which the company operates and security requirements it needs to fulfill. Then, this scope is documented and published to employees and other stakeholders. The Information Security inputs such as security policy, security manuel, security rules, vulnerabilities, threats, information classification criteria are defined based on this scope. Thus, it is ensured that all company operations are carried out with a focus on security objectives.

4.3. FRAMEWORK DEVELOPMENT

As discussed in literature review section we developed this methodological framework based on the ISO 27001 requirements to guide us during Information Security Management System implementation. Information Security Management System is a risk based system. Thus, Risk Management Process is in the center core of the system as it can be seen in the Figure 4.1.

The purpose of establishing this framework was to create a management system to ensure an organization’s information is protected secure against internal and external risks and to provide sustainability of this system.

In following section, each step of this framework will be explained in detail including individual process maps developed.

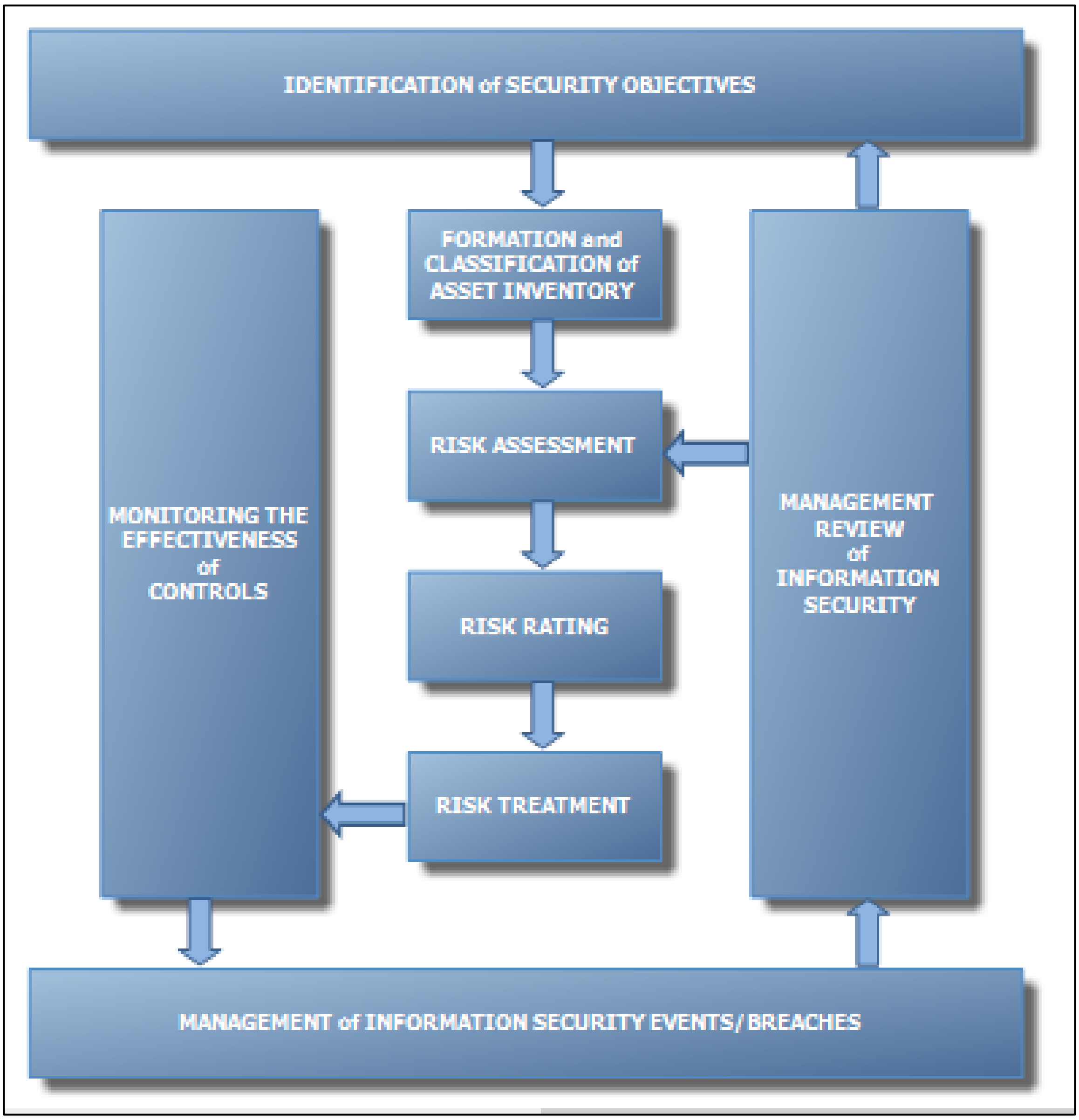

IDENTIFICATION of SECURITY OBJECTIVES
FORMATION and CLASSIFICATION of ASSET INVENTORY
RISK ASSESSMENT
RISK RATING
RISK TREATMENT
MONITORING THE EFFECTIVENESS of CONTROLS
MANAGEMENT REVIEW of INFORMATION SECURITY
MANAGEMENT of INFORMATION SECURITY EVENTS/ BREACHES

Figure 4.1. Information security management system methodological framework.

4.4. FORMATION AND CLASSICATION OF ASSET INVENTORY

Formation and classification of asset inventory is the fundamental step of risk analysis process.

An asset is any element which has value for an organization and consequently should be protected properly. People, information, software, hardware, building etc are considered as assets. The most intangible asset in the given examples is information. Information can be found everywhere in an organization. It can be processed by hardware and software, stored in media, written in documents and can take place in employee's mind or communications.

Therefore, only protecting the software, hardware, facility is not sufficient, it must be ensured that the employees don't share sensitive company information with third parties. Awareness trainings, signing NDA (Non-Disclosure Agreements) are important means to achieve this goal.

As ISO 27001 standard proposes, we categorized the assets in five classes as information, physical, software, service and process assets.

The term company information asset refers to all forms of information such as electronically generated, printed, filmed, typed, stored or verbally communicated. All the information circulating within the company evaluated in this class. This information may be held in the library, in the company's business processes or in employees' mind in various forms. Databases like customer, sales, marketing information, data files and printed materials, all procedures and archived information fall into this class. In our study, information assets are divided into 4 subcategories as database like servers, data file like records on fileserver, printed material like purchase contract and other for any information which does not fit into these 3 subcategories.

To ensure the proper protection and usage of information assets, information confidentiality levels are determined. As ISO 27001 standard suggests, in this methodology 4 confidentiality levels (Secret, Confidential, Internal Use Only and Public) are used (These levels are for only information assets).

Table 4.1. Information confidentiality levels.

INFORMATION CONFIDENTIALITY LEVELS	
SECRET	Information with controlled numbered circulation, hand delivered and not to be disclosed outside without specific approval of the executive committee or the managing director of the relevant entity, as otherwise such unauthorized disclosure could cause serious danger to the interests of the company. They are the most critical informations, only administration staff can access them. It is very important for the company not to access without authorization, reveal or not to share.
CONFIDENTIAL	Information circulated internally only on a need to know basis or with specific distribution lists. Not to be disclosed externally except by approval of company management and must be supported by a valid Non Disclosure Agreement (NDA), as otherwise such unauthorized disclosure could be prejudicial to the interests of the company or its staff. Personal information has always to be handled in a confidential manner, in accordance with local laws and regulations; in addition, it should be marked as "Personal and Confidential".
INTERNAL	Items containing information that may be shared freely inside the Group but that must not be disclosed outside the group without authorization from a department/company manager and must be supported by a valid Non Disclosure Agreement (NDA), as otherwise such unprotected disclosure could cause some damage to the company.
PUBLIC	Information already known to be in the public domain. Copyright restrictions may still apply. Information used by the company that is also available in the public domain.

Table 4.1 depicts the policies for the usage, distribution and protection of information belonging to each confidentiality level based upon its sensitivity, value and criticality to the

organization. Employees take the confidentiality level into consideration while they are using or distributing any company information. For example, if an information asset is labeled as “Internal Use Only” they shouldn’t share this information with third parties. The level of impact in case of any disclosure or security breach is directly proportionate to confidentiality level of information.

The term physical asset refers to any tangible asset that can process information such as computers, server rooms, mobile devices, production machines, fax, air conditioners etc. In our study, physical assets are divided into 5 subcategories as computer equipments like notebooks, communication equipments like mobile phones, recording media like backup cartridge, network equipments like ethernet switches, other for any physical asset (such as spare parts, fire extinguisher) which does not fit into these 4 subcategories.

The term software asset refers to various kinds of programs used to operate computers and other related devices. Any program that is installed on a computer or on any other device is software. Software enables computer to perform a specific task and provide an interaction between user and the computer. Without software, most computers would be unfunctional. For example, without any music player program like WinAmp you could not listen to music from your computer or without an Internet browser software like Mozilla Firefox you could not search in the internet. In our study, software assets are divided into 4 subcategories as operating system like Windows 8, application software like groundwork monitoring tool, system software like back up software, other for any software which does not fit into these 3 subcategories.

The term service asset refers to services that help to ensure the continuity of the information security management system. Most of this services are got from external authorized providers. For example ambient temperature and humidity of systems room is vital for continuous operation of servers. And there are acceptable ranges for systems room temperature and humidity. Small variations from these ranges can cause major disruption in the computer systems and therefore it is critical to keep these parameters under control. In order to ensure that the air conditioners working properly, periodical maintenance service is got from air conditioning company. In our study, service assets are divided into 5 subcategories as information services like software maintenance, communication services like GSM operator services, consulting services like management systems consultancy, technical services like uninterruptible power supply maintenance, other for any service asset (such as cleaning services, stuff transport services) which does not fit into these 4 subcategories.

The term process asset refers to all policies, procedures, guideliness and process maps which describe how the company activities are carried out. Since these activities are specific to the company and include know-how, it is very important to protect process assets in terms of competitive advantage. In our study, process assets are divided into 7 subcategories as strategic planning like strategic planning procedure, information management like document controlling procedure, resource management like human resources planning procedure, service management like customer services management procedure, improvement management like nonconformity and improvement management guideline, otomation process management like automatic bill payments, other for any process asset which does not fit into these 4 subcategories.

In Information Security Management System, asset management is an essential process since it determines ownership of all organizational assets. The assets are identified by doing an inventory of all assets such as software, physical assets (for instance, PCs, and system hardware), services (for instance, consultancy services), intangibles like the prestige and organizational image, and the information in the organization. The information can be found in everywhere in the organization, and can be in different forms. After the inventory, possession or accountability is assigned to all assets, and manuels are designed for acceptable use of the assets. The main aim of information classification is to make sure that information takes an proper level of preservation as regard to its cruciality to the organization [23].

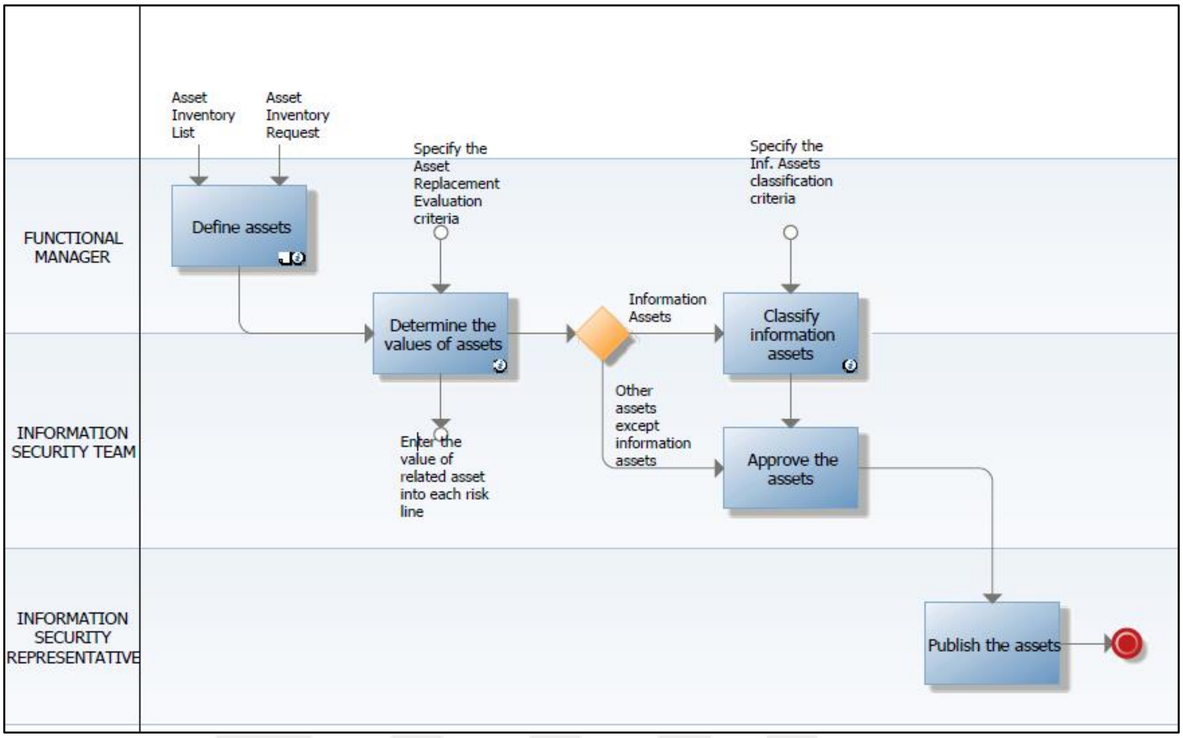

FUNCTIONAL MANAGER
INFORMATION SECURITY TEAM
INFORMATION SECURITY REPRESENTATIVE
Asset Inventory List
Asset Inventory Request
Define assets
Specify the Asset Replacement Evaluation criteria
Determine the values of assets
Enter the value of related asset into each risk line
Information Assets
Other assets except information assets
Specify the Inf. Assets classification criteria
Classify information assets
Approve the assets
Publish the assets

Figure 4.2. Formation and classifiaction of asset inventory process map.

The Figure 4.2 explains how the formation and classification of asset inventory process is carried out in our methodology.

As a first step of this process, all assets available in the organization are defined. In this step asset definition is done in a list which is called as asset inventory list. In this list, assets are added under 5 classes (information, physical, software, service and process assets). And each asset in this list must be defined with the parameters which are taken into account during risk analysis study; asset location, asset definition, asset owner, asset custodian, replacement value and asset confidentiality level (for only information assets).

A company asset may exist in a physical location or in an intangible place, so asset location can be expressed as a cabinet, a server room, a filepath, a database or a shared network drive. As every asset location has specific information security risk, this parameter is extremely important to decide on the measures to be taken in case of any accident, disaster or information security breach.

The parameter asset definition stands for a brief description of what the asset is and what it does. It also includes all components of the assets and other key information.

Asset owner is primarily responsible employee for the purpose of ensuring confidentiality, availability and integrity of the related asset. Asset owner is responsible for:

- Identifying the classification level of all corporate information within his/her organizational unit.
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity and availability of the information resource in accordance with company standards.
- Monitoring application of the safeguards within his/her organizational unit to ensure compliance and reporting non-compliance.
- Authorizing access for those who have a business need for the information.
- Removing access from those who no longer have a business need for the information.

Asset custodian is responsible for protecting the assets by implementation and maintenance of preservations established by asset owner.

After all assets defined with asset location, asset definition, asset owner, asset custodian parameters in asset inventory list, asset valuation criteria is determined. In our study this criteria is based on the replacement value of the asset. Replacement value of an asset refers to the cost incurred, in case of any damage or destruction of an asset, for the substitution of it with a similar asset. While it is easy to assign a quantitative value to a tangible asset like a machine, it is quite difficult to do it for an intangible asset like brand. For example, in case of any damage to the brand, loss of marketshare is predicted and the value of brand is assigned according to this value.

Table 4.2. Asset valuation table.

ASSET VALUATION	
RATING (Asset Value)	COST RANGE
1	0-50.000$
2	50.001-150.000 $
3	>150.000 $

The Table 4.2 demonstrates the values of assets as rating (1, 2, 3) based on the cost (replacement value) range. The cost range criteria and corresponding ratings may vary depending on the company size, field of operations etc.

The next action is classifying information assets based on the confidentiality level criteria, as secret, confidential, internal or public. As it is discussed previously, this classifation done for only information assets. These classified information assets and other assets is approved by information security team and published by information security representative.

All the parameters defined in formation and classification of asset inventory process are used in the risk analysis process.

4.5. RISK ANALYSIS

Any organization must adopt to new information technology resources to get competitive advantage and achieve its strategic objectives. However, these technologic resources create some security risks. So, an information security risk analysis is essential to properly protection of the organization’s information assets.

Risk is the possibility that a threat misuses a vulnerability of an information asset, causing a harm to information management system in terms of confidentiality, integrity and availability. As an example, the collapse of the system in a building (risk) without lightning rod (vulnerability), as a result of lightning (threat). Below we will define the terms vulnerability/threat in detail and state the common vulnerabilities/threats specified in the ISO 27001 standard.

Vulnerability is a weakness that might be exploited due to lack of control on an asset. For example, if operating system security updates are not done, this means that there is a weakness in the operating system.

Common vulnerabilities defined in the ISO 27001 Standard are below:

- Sensitive hardware
- Lack of periodic maintenance
- Lack of controls
- Incompetent personnel
- Undefined processes
- Lack of records
- Inappropriate/insufficient hardware
- Inappropriate/insufficient software
- Complicated process
- Lack of communication
- Lack of documentation
- Incorrect parameter set up
- Lack of access control
- Lack of contract administration (NDA/SLA)
- Insufficient back-up system
- Inappropriate facility
- Lack of personnel
- Unclear duties and responsibilities
- Wrong classification of information
- Legislative non-compliance

Threat is an element that may cause harm on an information asset in terms of one or more information security attributes (Confidentiality, Integrity, Availability). Sometimes it can be natural threats like earthquake, lightning etc, sometimes it can be environmental threats like power cut, leakage or human-driven threats such as bad data input, unauthorized access, network blitz etc.

Common threats defined in the ISO 27001 Standard are below:

- Physical damage
- Natural events
- Loss of essential services
- Disturbance due to thermal radiation
- Compromise of information
- Technical failures
- Unauthorised actions
- Process/Organization
- Compromise of functions
- Incorrect operation
- Corruption of data

Risk analysis study is carried out by taking into consideration the factors such as threats, vulnerabilities, controls, security requirements, information assets and their values.

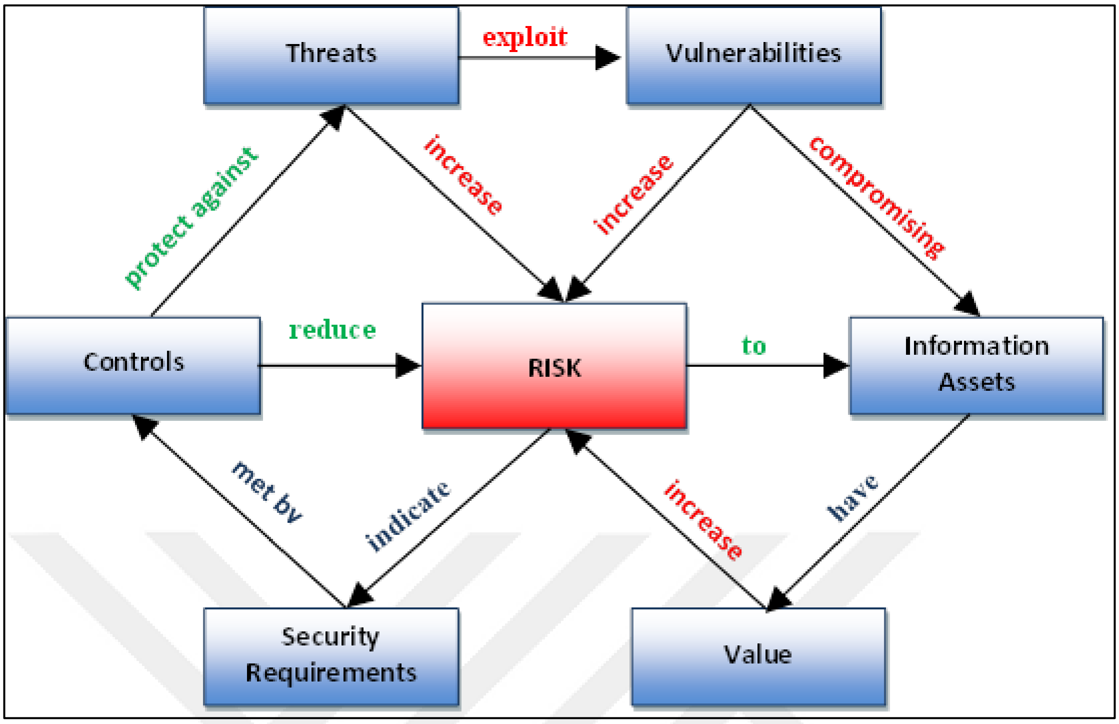


Figure 4.3. Risk interaction scheme.

The interaction among these factors is illustrated in the Figure 4.3. As shown in the scheme threats and vulnerabilities are risk-increasing factors and risk occurs when a threat exploits a vulnerability. Vulnerabilities also may lead to compromise of an information asset and the greater the value of the asset, the higher the risk. In order to minimize this risk, security requirements must be satisfied by the proper controls. These controls protects the information assets against the threat and the possibility of its explotation of the related vulnerability, thus the risk decreases. Risk analysis process is performed based on the interactions among these factors.

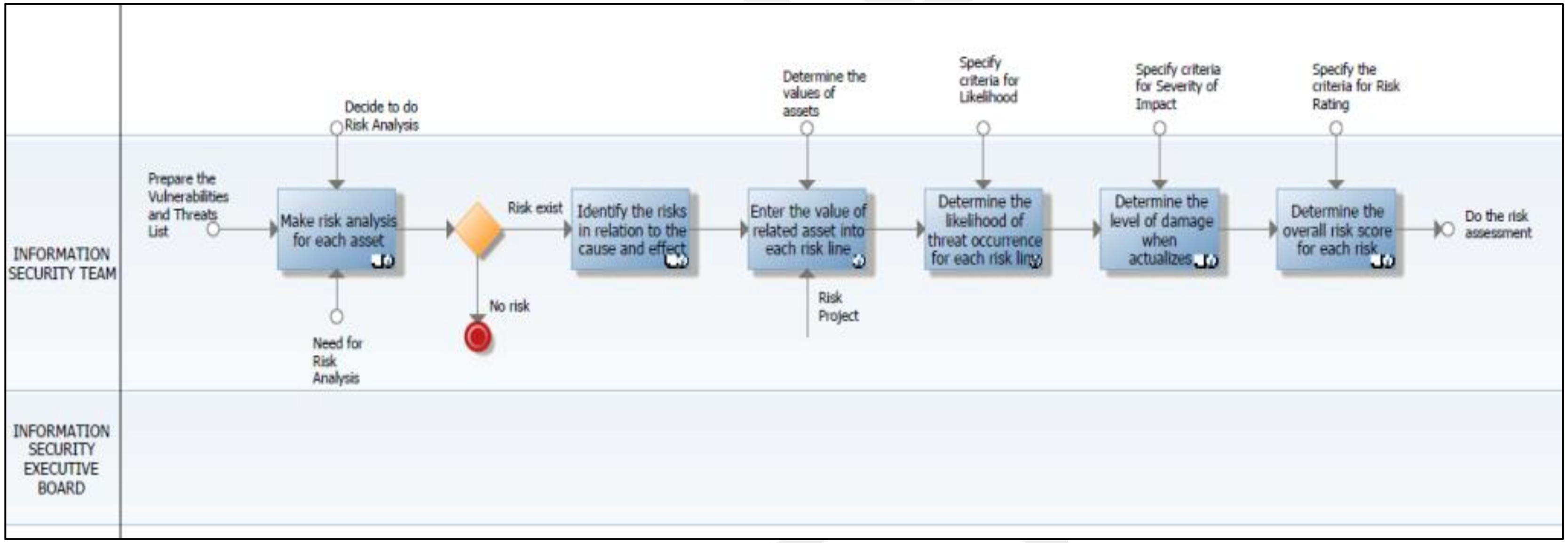
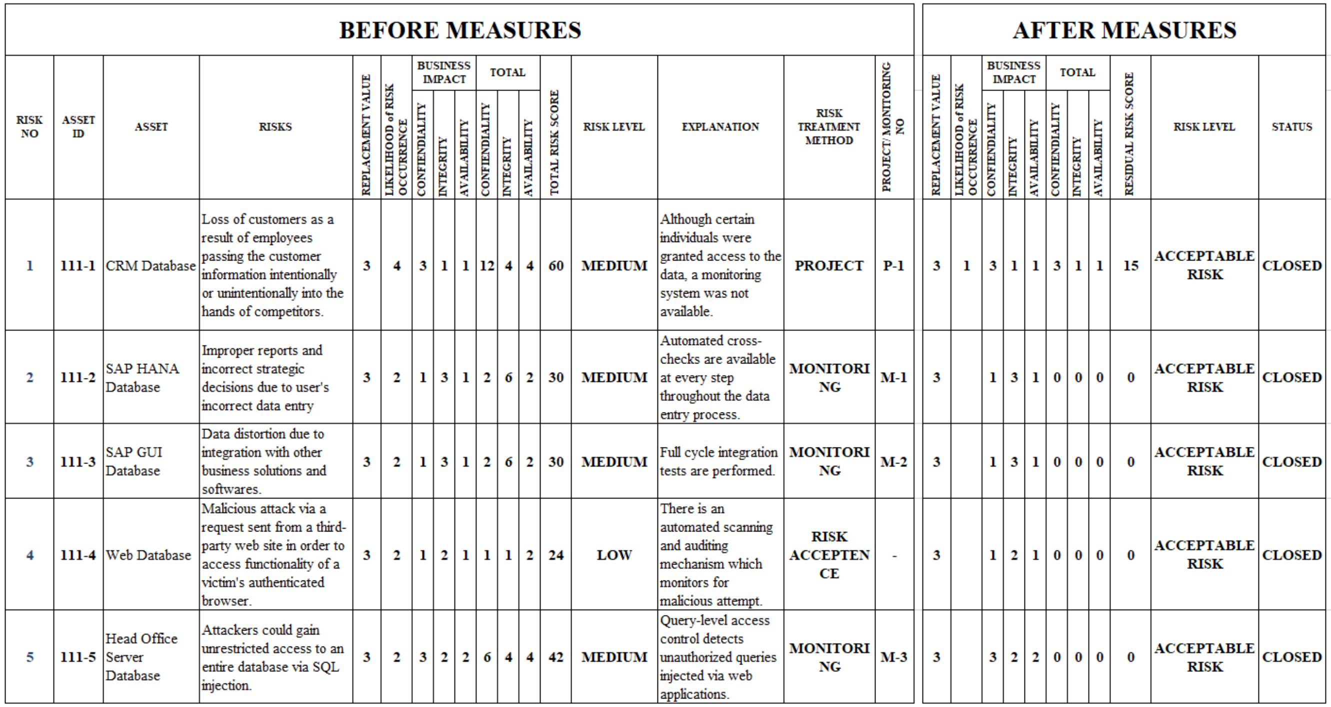

INFORMATION SECURITY TEAM
INFORMATION SECURITY EXECUTIVE BOARD
Prepare the Vulnerabilities and Threats List
Decide to do Risk Analysis
Make risk analysis for each asset
Need for Risk Analysis
Risk exist
No risk
Identify the risks in relation to the cause and effect
Determine the values of assets
Enter the value of related asset into each risk line
Risk Project
Specify criteria for Likelihood
Determine the likelihood of threat occurrence for each risk line
Specify criteria for Severity of Impact
Determine the level of damage when actualizes
Specify the criteria for Risk Rating
Determine the overall risk score for each risk
Do the risk assessment

Figure 4.4. Risk analysis process map.

As it seen in Figure 4.4, as the first step of this process, risk analysis is performed for each asset defined in the asset inventory list which is created in the Formation and Classification of Asset Inventory Process. The Risk Analysis table is used in this process.

Table 4.3. Risk analysis table.



BEFORE MEASURES																	AFTER MEASURES										
RISK NO	ASSET ID	ASSET	RISKS	REPLACEMENT VALUE	LIKELIHOOD of RISK OCCURRENCE	BUSINESS IMPACT			TOTAL			TOTAL RISK SCORE	RISK LEVEL	EXPLANATION	RISK TREATMENT METHOD	PROJECT/ MONITORING NO	REPLACEMENT VALUE	LIKELIHOOD of RISK OCCURRENCE	BUSINESS IMPACT			TOTAL			RESIDUAL RISK SCORE	RISK LEVEL	STATUS
						CONFIENDIALITY	INTEGRITY	AVAILABILITY	CONFIENDIALITY	INTEGRITY	AVAILABILITY								CONFIENDIALITY	INTEGRITY	AVAILABILITY	CONFIENDIALITY	INTEGRITY	AVAILABILITY			
1	111-1	CRM Database	Loss of customers as a result of employees passing the customer information intentionally or unintentionally into the hands of competitors.	3	4	3	1	1	12	4	4	60	MEDIUM	Although certain individuals were granted access to the data, a monitoring system was not available.	PROJECT	P-1	3	1	3	1	1	3	1	1	15	ACCEPTABLE RISK	CLOSED
2	111-2	SAP HANA Database	Improper reports and incorrect strategic decisions due to user's incorrect data entry	3	2	1	3	1	2	6	2	30	MEDIUM	Automated cross-checks are available at every step throughout the data entry process.	MONITORING	M-1	3		1	3	1	0	0	0	0	ACCEPTABLE RISK	CLOSED
3	111-3	SAP GUI Database	Data distortion due to integration with other business solutions and softwares.	3	2	1	3	1	2	6	2	30	MEDIUM	Full cycle integration tests are performed.	MONITORING	M-2	3		1	3	1	0	0	0	0	ACCEPTABLE RISK	CLOSED
4	111-4	Web Database	Malicious attack via a request sent from a third-party web site in order to access functionality of a victim's authenticated browser.	3	2	1	2	1	1	1	2	24	LOW	There is an automated scanning and auditing mechanism which monitors for malicious attempt.	RISK ACCEPTENCE	-	3		1	2	1	0	0	0	0	ACCEPTABLE RISK	CLOSED
5	111-5	Head Office Server Database	Attackers could gain unrestricted access to an entire database via SQL injection.	3	2	3	2	2	6	4	4	42	MEDIUM	Query-level access control detects unauthorized queries injected via web applications.	MONITORING	M-3	3		3	2	2	0	0	0	0	ACCEPTABLE RISK	CLOSED

The Table 4.3 is the short version of risk analysis study, full version is in the Appendix A.

Table 4.3 includes the main inputs of risk analysis which are used in total risk score calculation such as replacement value, likelihood of risk occurrence, business impact in terms of information security attributes (Confidentiality, Integrity and Availability). This table consists of two parts; “Before the Measures Are Taken” and “After the Measures Are Taken”. The “Before the Measures Are Taken” part is actually can be described as an assessment and during risk analysis process only this part is filled. Replacement value and business impacts of information security attributes will not change with the measures taken and therefore it is fixed for these two parts. The “After the Measures Are Taken” part can be described as a reassessment of the risks. And it is only filled if any project is implemented as a risk treatment method. All details will be explained under the caption of “4.7. Risk Treatment”.

If any risk exists on the related asset, the threat and vulnerability on the asset are entered into risk analysis table. Then the risk is identified in a way of cause and effect relationship considering which threat exploits which vulnerability of an asset at the same table. Next, the replacement value of each asset (which is determined in the Formation and Classifiaction of Asset Inventory Process) is entered at every single risk line. The following step is to determine the likelihood level of the risk occurrence and enter it to the risk analysis table. Mostly, this level is determined based on the frequency of occurrence at a certain time period. Thereby, the actual data from the past is very important in terms of determining this level accurately. Also, providing appropriate controls and ensuring their effectiveness decrease the likelihood level of risk occurrence. So, in addition to the historical data, if there are new security controls, they must be taken into consideration while determining this level.

Table 4.4. Likelihood of risk occurrence table.

LIKELIHOOD of RISK OCCURRENCE		
RATING	LIKELIHOOD	FREQUENCY
1	Very Low	Almost never
2	Low	Once in a year or only in abnormal situations
3	Mean	Few times in a year
4	High	Frequently (Once in a month)
5	Very High	Very Frequently (Everyday, once in a week)

The Table 4.4 demonstrates the likelihood level of risk occurrence as rating (1, 2, 3, 4, 5) based on the frequency of occurrence at a certain time period. As a next step, the total value of business impact (harm) in case of risk occurrence is determined and entered at the risk analysis table. The total value of business impact refers to the cost incurred in terms of business interruption, loss of competitive power, loss of reputation or any other direct costs when a risk occurs. Also, 3 fundamental attributes (Confidentiality, Integrity, Availability) are taken into account during this evaluation. For example, when availability of internet access of a dot com company is denied by a hacker, online shopping can not be done. This business interruption causes direct cost due to fixing the problem and being not able to make sell. Furthermore, customers lose trust in the company and shop from competitors, which means loss of competitive power and loss of reputation.

Table 4.5. Total value of business impact.

TOTAL VALUE of BUSINESS IMPACT **(CONFIDENTIALITY+INTEGRITY+AVAILABILITY)**		
RATING	COST RANGE (Direct+Indirect)	EVALUATION CRITERIA
1	0-50.000 $	Direct Cost Business Interruption Loss of competitive power Loss of reputation
2	50.001-150.000 $	
3	> 150.000 $	

The Table 4.5 demonstrates the total value of business impact as rating (1, 2, 3) based on the direct and indirect cost due to a risk occurrence.

As a last step of risk analysis process total risk score is calculated by multiplying replacement value and likelihood of occurrence value with the total (confidentiality impact+integrity impact+availability impact) value of business impact. The formula is below:

$$\begin{aligned} &Total\ Risk\ Score \\ &\quad = Asset\ (Replacement)\ Value\ Rating \\ &\quad \times \big[Likelihood\ of\ Risk\ Occurrence\ Rating \\ &\quad \times \big((Confidentiality + Integrity \\ &\quad + Availability) Business\ Impact\ Rating\big)\big] \end{aligned} \tag{4.1}$$

All the parameters in this formula have been gathered in risk analysis table and the total risk score is calculated automatically on the excel file. And the risk score is the main input of next process (Risk Assessment).

4.6. RISK ASSESSMENT

Risk assessment is a critical step of ISMS which helps the risk treatment process in terms of accurate controls against the risks, appropriate allocation of resources on these controls and proper prioritization of actions to mitigate the risks. The main purpose of this step is to rate the risks as high level, medium level and low level. To be able to do this rating a risk level matrix must be created based on the likelihood level and threat impact level.

Table 4.6. Risk level matrix.

RISK LEVEL MATRIX			
LIKELIHOOD LEVEL	**IMPACT LEVEL**		
	HIGH	MEDIUM	LOW
	3	2	1
VERY HIGH	HIGH	HIGH	MEDIUM
5	135	90	45
HIGH	HIGH	HIGH	MEDIUM
4	108	72	36
MEDIUM	HIGH	MEDIUM	MEDIUM
3	81	54	27
LOW	MEDIUM	MEDIUM	LOW
2	54	36	18
VERY LOW	MEDIUM	LOW	LOW
1	27	18	1

As it seen in the Table 4.6, there are 3 risk levels as High, Medium and Low. After this classification is done, corresponding total risk scores (which are calculated in risk analysis) are matched with these levels.

If the risk score is between 72 and 135 the risk is a high level risk, if it is between 27 and 71 the risk is a medium level risk and if it is between 1 and 26 the risk is a low level risk.

Risk assessment process is performed based on these risk level matrix.

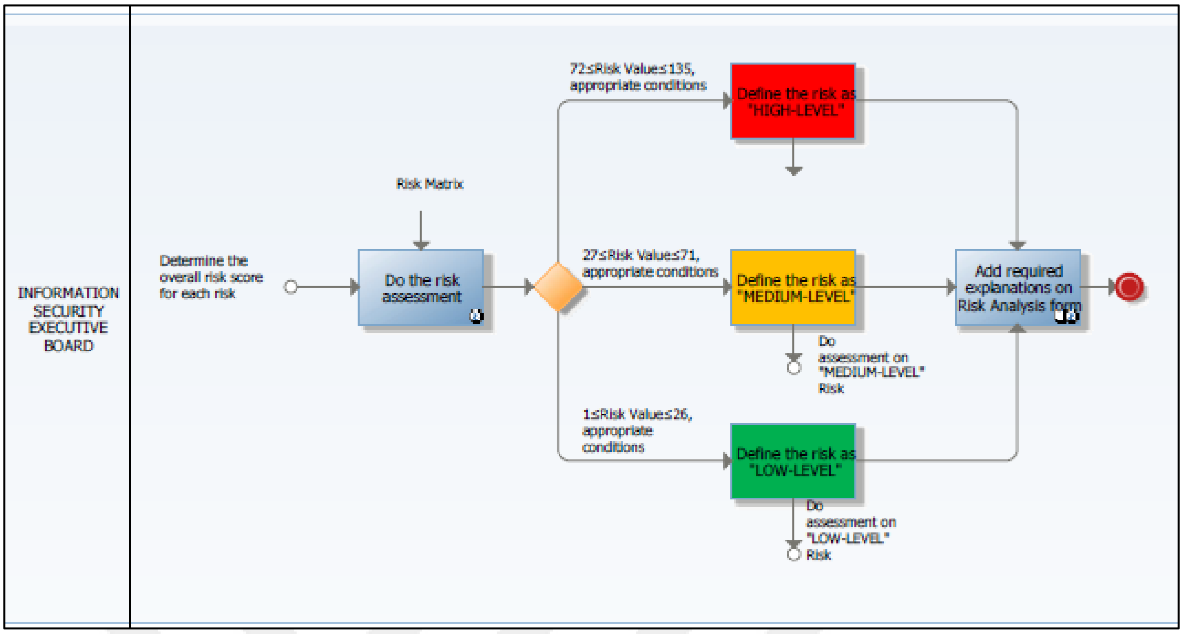

INFORMATION SECURITY EXECUTIVE BOARD
Determine the overall risk score for each risk
Risk Matrix
Do the risk assessment
72≤Risk Values≤135, appropriate conditions
Define the risk as "HIGH-LEVEL"
27≤Risk Values≤71, appropriate conditions
Define the risk as "MEDIUM-LEVEL"
Do assessment on "MEDIUM-LEVEL" Risk
1≤Risk Values≤26, appropriate conditions
Define the risk as "LOW-LEVEL"
Do assessment on "LOW-LEVEL" Risk
Add required explanations on Risk Analysis form

Figure 4.5. Risk assessment process map.

After determining the overall risk score for each risk in risk analysis process, risk assessment is done as described in Figure 4.5. Risk assessment refers to determination of risk as “High Level”, “Medium Level” or “Low Level”. According to the risk level, explanation (this risk is assigned as low-level because there are sufficient controls so the likelihood of occurrence is low and risk score is under 26 etc) for each risk added on the risk analysis table (Table 4.3).

Also, after risk assessment, the actions to be taken and urgencies of these actions are generalized based on each risk level (risk score interval).

Table 4.7. Action/urgency matrix for each risk level.

ACTION/URGENCY MATRIX	
RISK SCORE INTERVAL	ACTION/URGENCY
72-135	UNACCEPTABLE RISK
	Improvement project should be done immediately and level of risk should be decreased.
27-71	REMARKABLE RISK
	Should be controlled and monitored.
1-26	ACCEPTABLE RISK
	Additional precaution of monitoring activity is not necessary under appropriate conditions.

As it is seen in the Table 4.7, for high level risks, corrective measures must be determined. Even if the existing system works, required measures and implementations should be determined as quickly as possible. A high level risk is unacceptable, it must be reduced to medium level or low level.

A medium level risk is qualified as remarkable risk. Corrective measures must be determined and implementation plans should be prepared.

A low level risk is considered as an acceptable risk. It must be determined by the system owner whether any measures will be taken or not. If it is decided to take no measure, then the risk can be accepted as is.

The risk treatment process is mainly carried out based on the Action/Urgency Matrix.

4.7. RISK TREATMENT

Risk treatment refers to actions such as implementing a project in order to reduce the level of information security risks, risk avoidance, risk transfer and risk acceptance. Selecting one of these risk response method depends on the risk score.

Depending on the risk score or level of the risk there are five kinds of risk treatment methods:

- Project can be implemented for all kind of risks to eliminate the risk or to decrease the level of risk. If it is decided to implement of a project to mitigate any risk, the residual risk score is calculated after all actions of projects are completed. Residual risk is defined as the remaining risk after project implementation. Project actions may only mitigate the likelihood of risk occurrence and the other parameters such as replacement value and business impact remains the same as in the “Before the Measures Are Taken” part of the Table 4.3. Thus, after project implementation, the new likelihood of risk occurrence rating is determined and entered into the “After the Measures Are Taken” part of the Table 4.3 on the related risk line. The residual risk score is calculated automatically in the excel file like “The Total Risk Score”. If the residual risk score is still at an unacceptable level a new improvement project must be implemented.
- Risk monitoring is the process in which identified risks are tracked, residual risks are monitored, new risks are identified. Risk response plans executed and effectivenes of controls are evaluated continuously. Risk monitoring is not applicable for high level risks, it is only for medium or low level risks. Monitoring system can be formed for existing controls to keep the risk at current level and for new controls to improve the process.
- Risk avoidance is eliminating the causes of the risk. For example, not installing a software which creates a potential risk. Risk avoidance is not applicable for high level risks, it is only for medium or low level risks.
- Transferring the risk to others (for example taking out a policy) in order to cover the losses incurred in case of the realization of a risk. Risk transfer is not applicable for high level risks, it is only for medium or low level risks.
- Accepting the risk as it stands and leave as it is. This response method is applicable for only low level risk.

Table 4.8. Risk treatment methods based on the risk level.

	HIGH LEVEL RISK	**MEDIUM LEVEL RISK**	**LOW LEVEL RISK**
PROJECT	√	√	√
MONITORING	X	√	√
RISK AVOIDANCE	X	√	√
RISK TRANSFER	X	√	√
RISK ACCEPTANCE	X	X	√

Table 4.8 summarizes which types of methods should be adopted for each level of risk.

4.7.1. Low Level Risk Treatment

As it is discussed under the caption of 4.6 Risk Assessment, Low Level Risks are characterised as acceptable risks. In this methodology low level risk score range is 1-26.

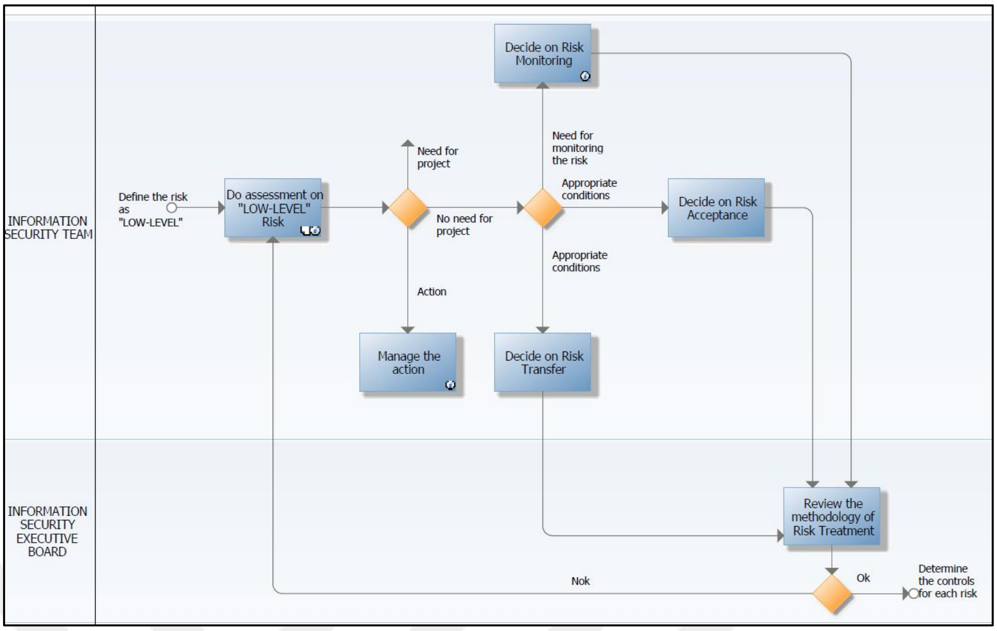

INFORMATION SECURITY TEAM
INFORMATION SECURITY EXECUTIVE BOARD
Define the risk as "LOW-LEVEL"
Do assessment on "LOW-LEVEL" Risk
Need for project
No need for project
Action
Manage the action
Decide on Risk Monitoring
Need for monitoring the risk
Appropriate conditions
Appropriate conditions
Decide on Risk Acceptance
Decide on Risk Transfer
Review the methodology of Risk Treatment
Nok
Ok
Determine the controls for each risk

Figure 4.6. Low level risk treatment process map**.**

The Figure 4.6 explains how the low level risk treatment process is carried out in our methodology.

As a first step of this process, low level risk is evaluated in more detail by Information Security Team in order to decide on the best fit risk treatment method. There are 3 possible decisions. If there is a need for a project, the demand is transmitted to project team and initiated. The second possible decision is to take a single action and the last one may be no need for a project or any action. If the last choice is preferred then we need to use one of risk monitoring, risk transferring, risk avoidance or risk acceptence alternatives as a risk treatment method.

Altough the level of risk is low, it may not be possible to choose risk transfer, risk avoidance or risk acceptance options, if there is a situation contrary to laws, customer contracts and corporate policies.

At the end of this process information security executive board review the methodology of low level risk treatment, if the assigned risk treatment method is sufficient, the controls for each risk are determined as a first step of next process (4.8 Monitoring the Effectiveness of Controls) and if it is unsatisfying, low level risk treatment process must be executed again.

4.7.2. Medium Level Risk Treatment

As it is discussed under the caption of 4.6 Risk Assessment, Medium Level Risks are characterised as remarkable risks. In this methodology medium level risk score range is 27-71.

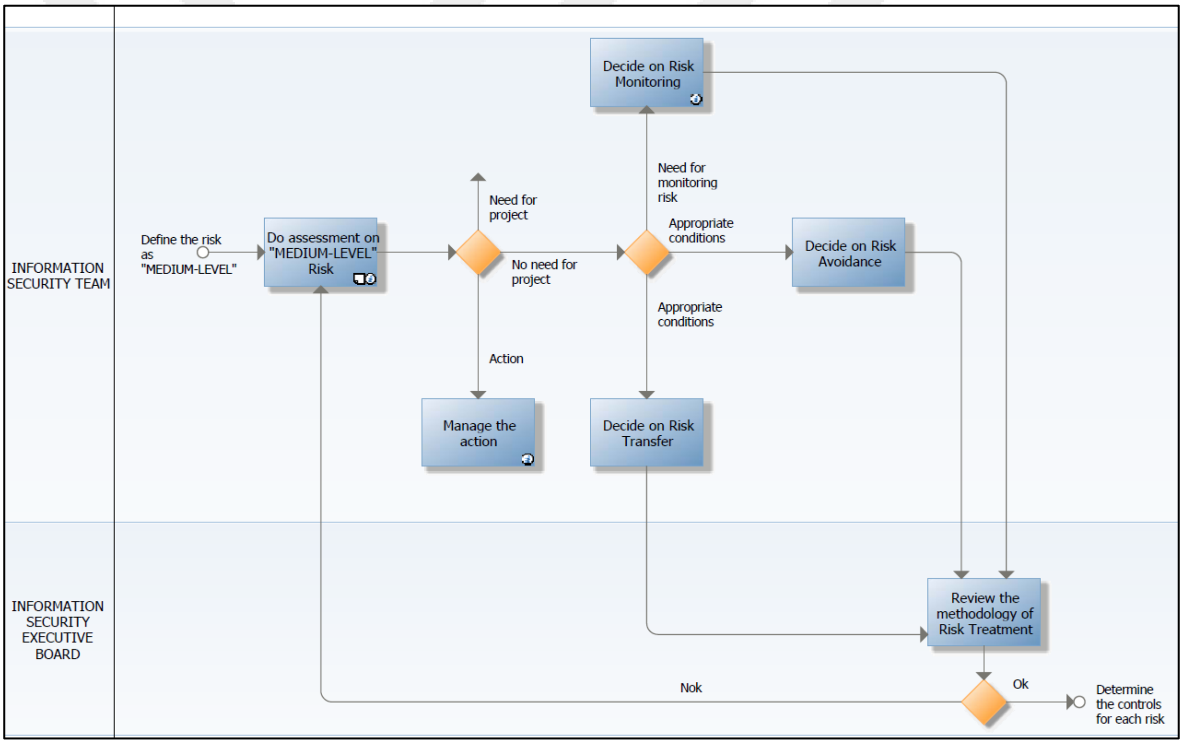

INFORMATION SECURITY TEAM
INFORMATION SECURITY EXECUTIVE BOARD
Define the risk as "MEDIUM-LEVEL"
Do assessment on "MEDIUM-LEVEL" Risk
Need for project
No need for project
Action
Manage the action
Decide on Risk Monitoring
Need for monitoring risk
Appropriate conditions
Decide on Risk Avoidance
Appropriate conditions
Decide on Risk Transfer
Review the methodology of Risk Treatment
Nok
Ok
Determine the controls for each risk

Figure 4.7. Medium level risk treatment process map.

The Figure 4.7 explains how the medium level risk treatment process is carried out in our methodology.

As a first step of this process, medium level risk is evaluated in more detail by Information Security Team in order to decide on the best fit risk treatment method. There are 3 possible decisions. If there is a need for a project, the demand is transmitted to project team and initiated. The second possible decision is to take a single action and the last one may be no need for a project or any action. If the last choice is preferred then we need to use one of risk monitoring, risk transferring or risk avoidance alternatives as a risk treatment method.

Altough the level of risk is medium, it may not be possible to choose risk transfer, risk avoidance options, if there is a situation contrary to laws, customer contracts and corporate policies.

At the end of this process information security executive board review the methodology of medium level risk treatment, if the assigned risk treatment method is sufficient, the controls for each risk are determined as a first step of next process (4.8 Monitoring the Effectiveness of Controls) and if it is unsatisfying, medium level risk treatment process must be executed again.

As it can be seen, risk treatment methodology is nearly the same for low level and medium level except risk acceptance option. Risk acceptance is only applicable for low level risks.

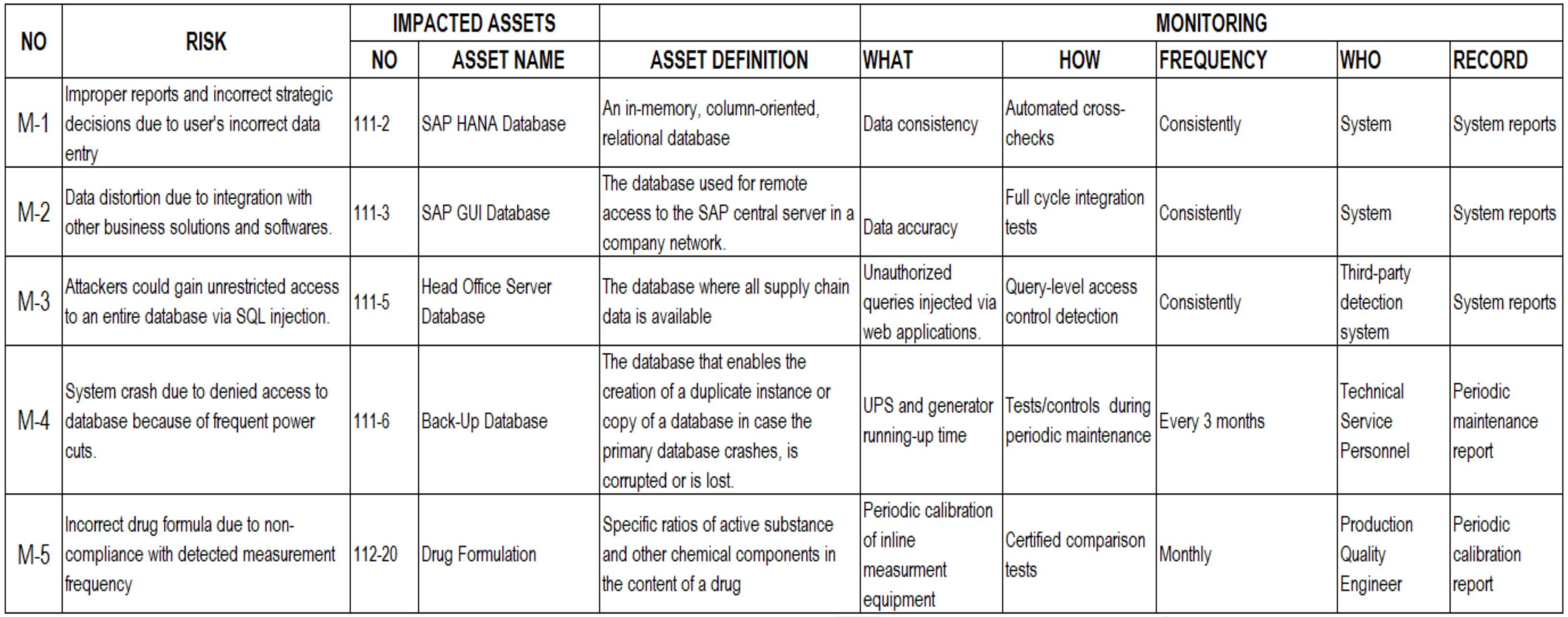
4.7.3. High Level Risk Treatment

High level risks require improvement projects with emergency action plan. As it is seen in the Table 4.8 risk monitoring, avoidance, transfer and acceptance can not be applied at high level risks. Such risks must be decreased to medium or low level by implementing a project, and then risk treatment methods can be applied.

4.8. MONITORING THE EFFECTIVENESS OF CONTROLS

After determining the risk treatment method for each risk, there may be need to prepare a control monitoring plan for some of the risks which should be controlled continuously or periodically. Control Monitoring Plan is formed in order to observe the efficiency of chosen controls for medium level risks and low level risks. The main purpose of this plan is to start corrective actions immediately, in case of any deviation from the required security conditions.

Table 4.9. Control efficiency monitoring plan.



NO	RISK	IMPACTED ASSETS			MONITORING				
		NO	ASSET NAME	ASSET DEFINITION	WHAT	HOW	FREQUENCY	WHO	RECORD
M-1	Improper reports and incorrect strategic decisions due to user's incorrect data entry	111-2	SAP HANA Database	An in-memory, column-oriented, relational database	Data consistency	Automated cross-checks	Consistently	System	System reports
M-2	Data distortion due to integration with other business solutions and softwares.	111-3	SAP GUI Database	The database used for remote access to the SAP central server in a company network.	Data accuracy	Full cycle integration tests	Consistently	System	System reports
M-3	Attackers could gain unrestricted access to an entire database via SQL injection.	111-5	Head Office Server Database	The database where all supply chain data is available	Unauthorized queries injected via web applications.	Query-level access control detection	Consistently	Third-party detection system	System reports
M-4	System crash due to denied access to database because of frequent power cuts.	111-6	Back-Up Database	The database that enables the creation of a duplicate instance or copy of a database in case the primary database crashes, is corrupted or is lost.	UPS and generator running-up time	Tests/controls during periodic maintenance	Every 3 months	Technical Service Personnel	Periodic maintenance report
M-5	Incorrect drug formula due to non-compliance with detected measurement frequency	112-20	Drug Formulation	Specific ratios of active substance and other chemical components in the content of a drug	Periodic calibration of inline measurment equipment	Certified comparison tests	Monthly	Production Quality Engineer	Periodic calibration report

The Table 4.9 is the short version of control efficiency monitoring plan, full version is in the Appendix B.

As it seen in the Table 4.9 control efficieny monitoring plan involves monitoring responsibilities with details like “Who will monitor what, how, how often and which records are created in order to prove these monitoring plan is followed etc”.

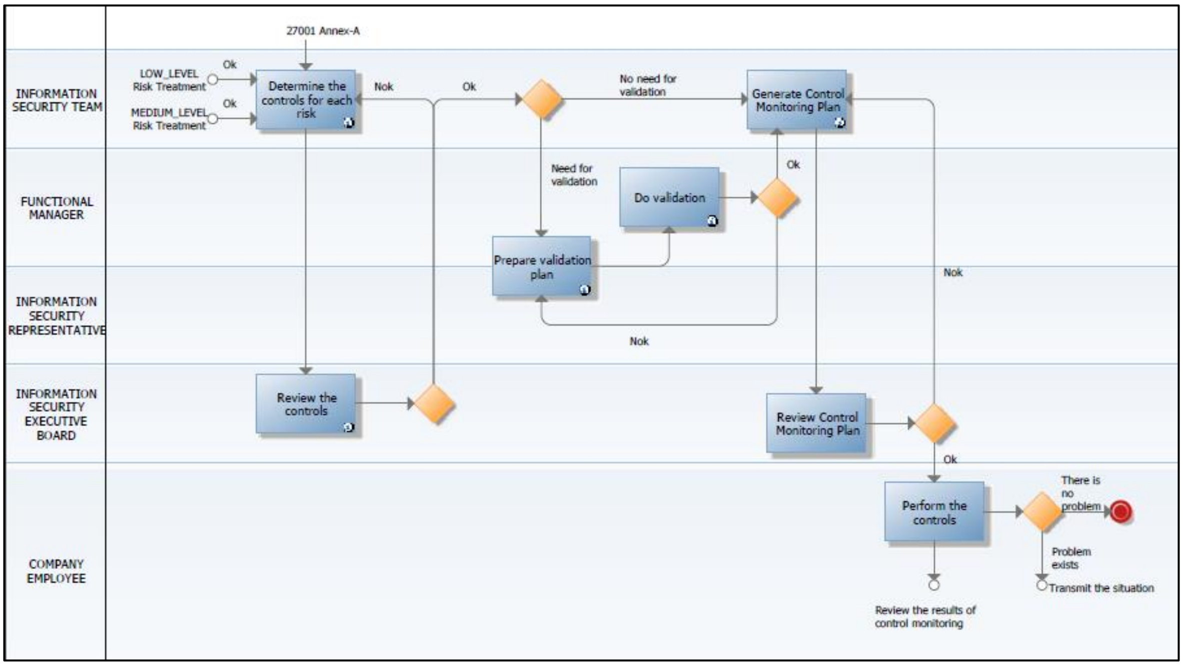

27001 Annex-A
INFORMATION SECURITY TEAM
LOW_LEVEL Risk Treatment
Ok
MEDIUM_LEVEL Risk Treatment
Ok
Determine the controls for each risk
Nok
Ok
No need for validation
Generate Control Monitoring Plan
FUNCTIONAL MANAGER
Need for validation
Do validation
Ok
Prepare validation plan
INFORMATION SECURITY REPRESENTATIVE
Nok
Nok
INFORMATION SECURITY EXECUTIVE BOARD
Review the controls
Review Control Monitoring Plan
Ok
COMPANY EMPLOYEE
Perform the controls
There is no problem
Problem exists
Transmit the situation
Review the results of control monitoring

Figure 4.8. Monitoring the effectiveness of controls process map.

The Figure 4.8 explains how the monitoring the effectiveness of controls process is carried out in our methodology.

As a first step of this process, by utilising Annex-A part of ISO 27001 standard, Information Security Team determine the controls for each risk and Information Security Executive Board review and approve the controls. Information Security Team decide on whether there is a need for validation or not. If it is needed, validation plan is prepared together with the relevant functional manager and information security representative. Subsequently functional manager does the validation. Information Security Team generate the Control

Monitoring plan to measure the efficiency of the controls. After the approval of this plan by information security executive board, relevant company employee perform the controls.

4.9. MANAGEMENT OF INFORMATION SECURITY EVENTS/BREACHES

All processes from 4.6 risk assessment to 4.8 monitoring the effectiveness of controls are carried out for current risks of the organizations. However, as all organizations are like living organisms, there might be new potential risks as the system operates. The changes like newly added processes, systems, machines, legislative regulations etc may cause new information security events/breaches and may rise new risks which are not taken into consideration in previous risk analysis study. The management of such risks are explained under this caption.

Information security event/breach indicates a single or a series of unexpected issues which are most likely to endanger the business operations and threaten the information security.

An information security event is defined as “change of state” in a system, environment, process, workflow or person. Every change brings along new risks. So they must be managed consistently in a living organization.

Examples for IS Events:

- Sofware updating
- Natural disasters (earthquake, flood etc)
- New business process
- New system user

An information security breach is usually a human-caused, malicious event that may lead to a significant disruption of business.

Examples for IS Breaches:

- Unauthorized access to common areas or services
- Service interruptions provided by IT
- Improper use of the Internet or E-mail
- Keeping company documents in unprotected places, or loss of them
- Not destroying the secret company document by an appropriate method
- Storing security records in insecure environments
- Data losses from computers
- Leaks or failures on company's communications infrastructure
- Leaving important or secret documents on the desk
- Leaving without locking the session

These events/breaches may also cause high impacts like closing down the business as it may cause mild effects for the company. So, the proper management of information security events/breaches is very critical in terms of detecting the problems immediately and taking related actions in a timely manner.

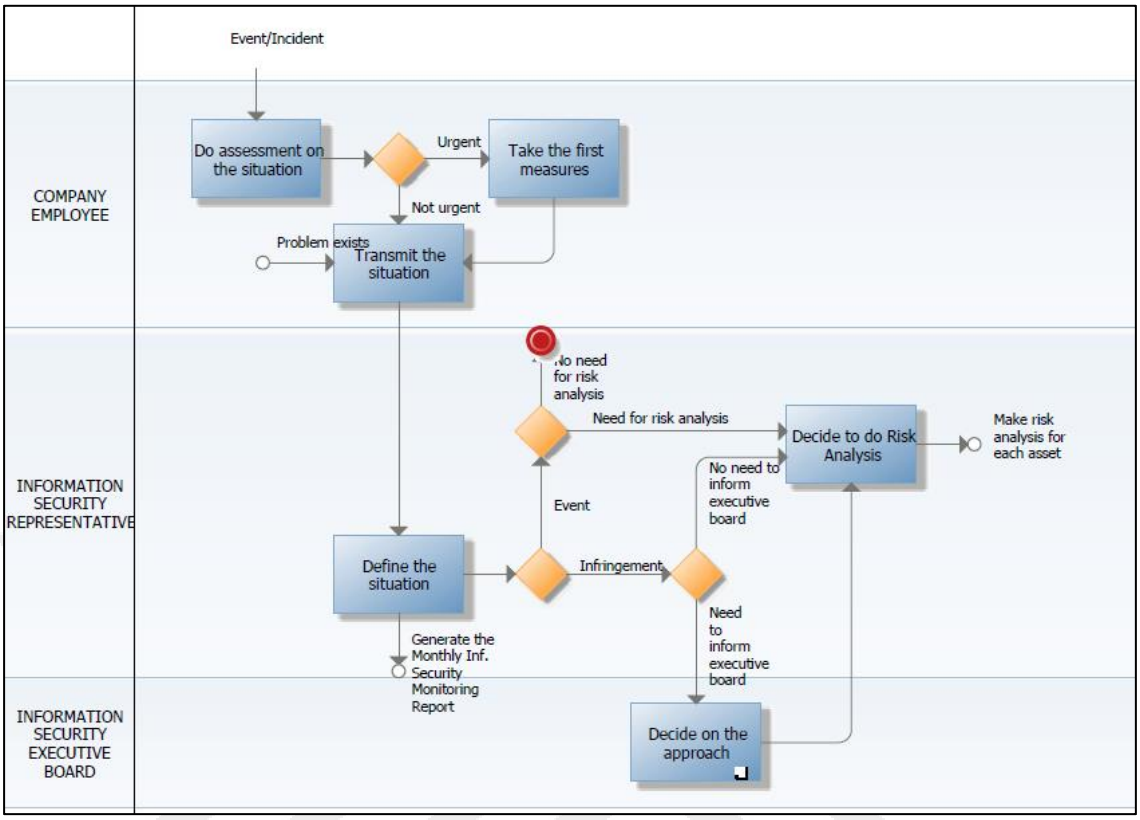

Event/Incident
COMPANY EMPLOYEE
Do assessment on the situation
Urgent
Take the first measures
Not urgent
Problem exists
Transmit the situation
INFORMATION SECURITY REPRESENTATIVE
No need for risk analysis
Need for risk analysis
Decide to do Risk Analysis
Make risk analysis for each asset
No need to inform executive board
Event
Define the situation
Infringement
Need to inform executive board
Generate the Monthly Inf. Security Monitoring Report
INFORMATION SECURITY EXECUTIVE BOARD
Decide on the approach

Figure 4.9. Management of information security events/breaches process map.

The Figure 4.9 explains how the management of information security events/breaches process is carried out in our methodology.

As it seen in the Figure 4.9, in case of any information security event or breach, relevant company employee asseses the severity of the situation. If the situation is urgent which requires emergency action, such as fire, theft etc, he/she directly takes the first measures and then transmits the situation to information security representative. If it is not an urgent situation he/she directly transmits the situation to information security representative to be evaluated.

Information security representative does situation assessment and decides if it is a security event or a breach. If it is a security event, doing risk analysis is optional based on the severity of effect on business, but if it is a security breach risk analysis is required. It is not needed to inform information security executive board for each security event or breach. Considering the financial cost on business due to the information security event or breach information security representative might inform information security executive board and board members may decide on the approach for the risk analysis. For example, it may be necessary to make an investment in order to eliminate related security event/breach, in this case the board decides whether this investment will be made or not.

4.10. MANAGEMENT REVIEW OF ISMS

As it is stated in the literature, management review of ISMS is essential for sustainability of the system. The main purpose of management review is to ensure that the Information Security Management System remains proper and effective, to discuss the opportunities to improve and comply with the changes such as new legal regulations, new business operations etc.

Information security representative and top management review the compliance, efficiency of the information security management system, functionality of risk management, at least once a year (Annual ISMS Management Review Meeting). In this meeting internal and external audit results are evaluated, corrective and preventive actions are determined. Also, top management evaluates risk acceptance criteria and resource requirements for sustainability and development of the existing system.

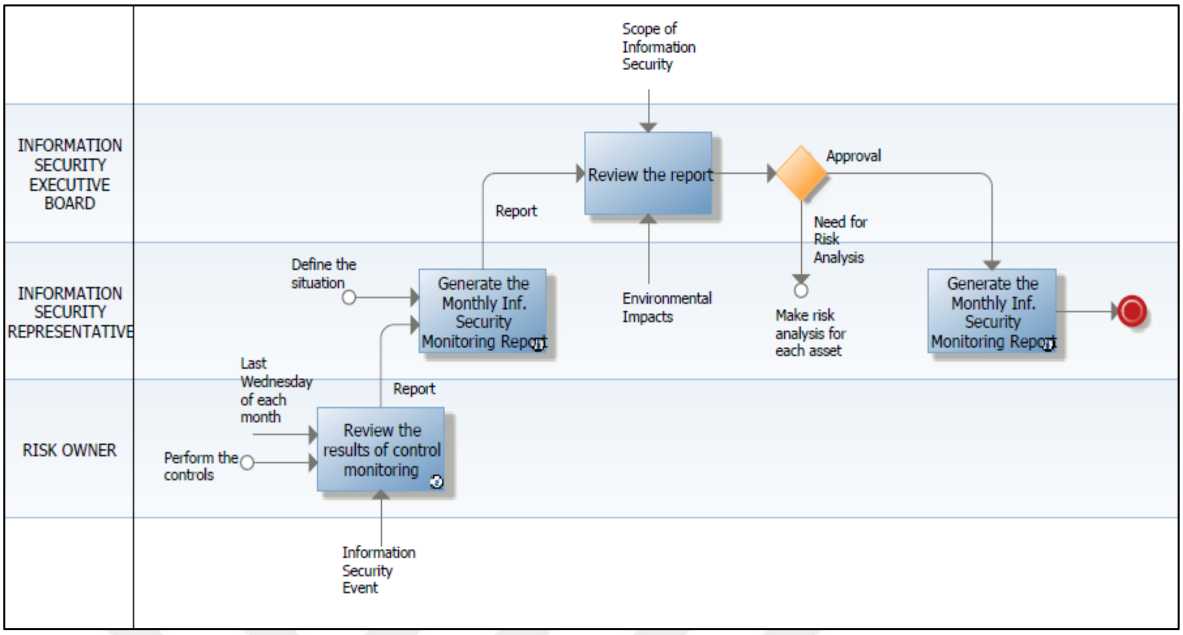

INFORMATION SECURITY EXECUTIVE BOARD
INFORMATION SECURITY REPRESENTATIVE
RISK OWNER
Scope of Information Security
Review the report
Approval
Report
Need for Risk Analysis
Define the situation
Generate the Monthly Inf. Security Monitoring Report
Environmental Impacts
Make risk analysis for each asset
Generate the Monthly Inf. Security Monitoring Report
Last Wednesday of each month
Report
Perform the controls
Review the results of control monitoring
Information Security Event

Figure 4.10. Management review of ISMS process map.

The Figure 4.10 explains how the management review of ISMS process is carried out in our methodology.

As a first step of this process, the risk owner reviews the results of control monitoring in accordance with 4.8 Monitoring the Effectiveness of Controls Process, and reports to Information Security Representative. He/she generates the Monthly Information Security Monitoring Report and submits it to Information Security Executive Board. The board evaluates the monitoring report. If the report is approved, Information Security Representative publishes it through the company. Otherwise, there is a need to make a new risk analysis for the related risks.

In conclusion, our information security management system methodology consists of these eight processes which are supported by ISO 27001 standard. In the next phase we will apply this methodology on a pharmaceutical company’s ISMS implementation.

5. APPLICATION

ABC Pharma Solutions was founded in 1971. It's line of business includes manufacturing and processing of drugs for many areas of medicine. The company exports finished products to several countries and also allocates a budget to its R&D activities and to produce new drugs. The company fights against counterfeit drugs and aims to protect its sensitive drug development data and formulas in order to maintain its competitive advantage. So, it is very essential to ensure information security for this company.

In this study, we used the developed framework to implement Information Security Management System (ISMS) at ABC Pharma Solutions.

5.1. IDENTIFICATION OF SECURITY OBJECTIVES

ABC Pharma Solutions Company's objective in establishing and implementing an Information Security Management System (ISMS) is to create an environment in which company information can be protected and maintained in terms of confidentiality, integrity and availability.

In our study we prepared information security management systems guidebook which is in accordance with our company objectives. ISMS guidebook includes information security objectives, rules, ISMS scope, vision, mission and policies, was prepared to inform all interested parties about the company's ISMS operations and follow the system requirements during their activities. We also, ensured that all company processes are carried out according to rules stated in this guidebook by making regular audits.

Also, we organized periodic awareness trainings in order to keep employees' interest alive and drew up personal NDA (Non-Disclosure Agreement) with them. Also, sanctions that they will face in case of any information security violation are stated in each employee's job description which is signed in the recruitment phase. Adoption of these kind of procedures improved the employees' contribution to ISMS and compliance with information security rules and objectives [20].

All company activities, projects and processes including outsourced services are within the scope of the ISMS.

5.2. FORMATION AND CLASSICATION OF ASSET INVENTORY

The Formation and Classification Asset Inventory process was carried out by following the steps shown in the Figure 4.2.

Table 5.1. Summary table of asset inventory.

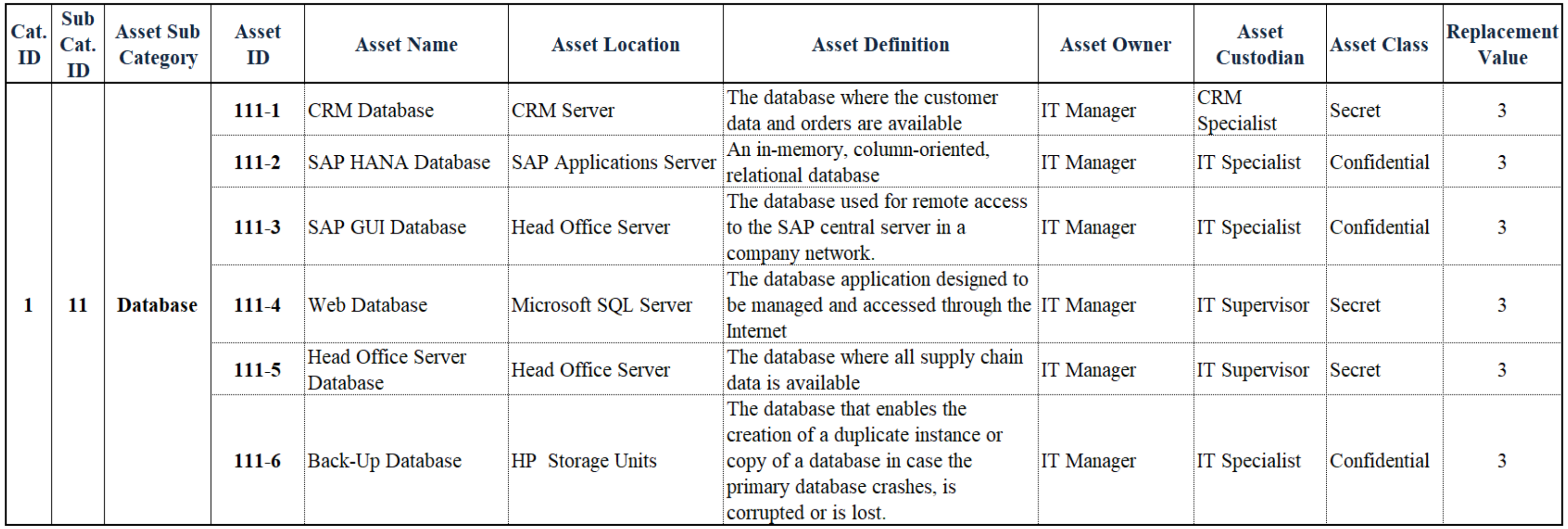
	Information Confidentiality Levels				
Type of Asset	Secret	Confidential	Internal Use Only	Public	Total Number of Assets
Information Assets	7	22	8	0	37
Physical Assets	x	x	x	x	31
Software Assets	x	x	x	x	19
Service Assets	x	x	x	x	17
Process Assets	x	x	x	x	18
Grand Total					122

As it can be seen in the Table 5.1, total number of assets defined was 122 (37 is information asset, 19 is physical asset, 31 is software asset, 17 is service asset and 18 is process asset).

These assets are shown in the Table 5.2 with parameters such as; asset location, asset definition, asset owner, asset custodian, replacement value and asset confidentiality level (for only information assets), as it is mentioned in the methodological framework part.

In our study we also prepared an asset classification policy based on ISO 27001 standard [5] and stated the responsibilities and rules on how to protect each category. Consequently, we ensured that any information asset receives an appropriate level of protection under the responsibility of right person(s) in accordance with its importance to our organization.

Table 5.2. Assets inventory table.



Cat. ID	Sub Cat. ID	Asset Sub Category	Asset ID	Asset Name	Asset Location	Asset Definition	Asset Owner	Asset Custodian	Asset Class	Replacement Value
1	**11**	**Database**	**111-1**	CRM Database	CRM Server	The database where the customer data and orders are available	IT Manager	CRM Specialist	Secret	3
			111-2	SAP HANA Database	SAP Applications Server	An in-memory, column-oriented, relational database	IT Manager	IT Specialist	Confidential	3
			111-3	SAP GUI Database	Head Office Server	The database used for remote access to the SAP central server in a company network.	IT Manager	IT Specialist	Confidential	3
			111-4	Web Database	Microsoft SQL Server	The database application designed to be managed and accessed through the Internet	IT Manager	IT Supervisor	Secret	3
			111-5	Head Office Server Database	Head Office Server	The database where all supply chain data is available	IT Manager	IT Supervisor	Secret	3
			111-6	Back-Up Database	HP Storage Units	The database that enables the creation of a duplicate instance or copy of a database in case the primary database crashes, is corrupted or is lost.	IT Manager	IT Specialist	Confidential	3

The Table 5.2 is the short version of assets inventory for each kind of assets (information, software, physical, service and process assets), full version is in the Appendix C-D-E-F-G.

After functional managers defined assets, they determined the values of assets together with information security team based on the criteria stated in the Table 4.2. They specified information confidentiality levels of information assets based on the criteria stated in the Table 4.1. 7 of information assets were set as secret, 22 were set as confidential, 8 were set as internal use only and 1 was set as public, which totals to 37 information assets out of total of 122 assests.

Next, Information Security Team approved these assets and Information Security Representative published the final inventory list companywide.

5.3. RISK ANALYSIS

ABC Pharma Solutions Company spends approximately $2 billion to devolop a typical kind of drug which also takes almost 10-15 years to launch to the market. So, there is a particular need for a precise risk analysis to protect drug recipes and intellectual property of the company.

Before risk analysis study we defined the vulnerabilities in terms of hardware, software, network, personnel, site and organization. Considering our information asset inventory we defined 85 types of vulnerabilities which are also included in the ISO 27001 standard [5].

Table 5.3. Summary table of vulnerabilities.

Vulnerability Area	**Number of Vulnerabilities**
Hardware	10
Software	23
Network	10
Personnel	8
Site	4
Organization	30
Total	85

Table 5.3 refers to the distribution of defined vulnerabilities according to their sources. These vulnerabilities are detailed in the Appendix H.

Then we defined the threats which may misuse the specified vulnerabilities and cause harm to the company's ISMS. The threats are defined in terms of physical damage, natural events, loss of essential services, disturbance due to thermal radiation, compromise of information, technical failures and unauthorised actions. Considering the specified vulnerabilities we defined 43 types of threats which are also included in the ISO 27001 standard [5].

Table 5.4. Summary table of threats.

Threat Type	Threats
Physical Damage	6
Natural Events	5
Loss of Essential Services	3
Disturbance due to Thermal Radiation	3
Compromise of Information	11
Technical Failures	5
Unauthorised Actions	5
Compromise of Functions	5
Total	43

Table 5.4 refers to the distribution of defined threats according to their types. These threats are detailed in the Appendix I.

After vulnerabilities and threats are defined risk analysis process was carried out by following the steps shown in the Figure 4.4.

Information security team determined the corresponding threats and vulnerabilities on the assets defined in the Table 5.2 and entered into the Table 4.3. Then they identified the risks on the assets, in cause effect relationship, based on the related vulnerabilities and threats. A total of 122 risks were defined. (All these risks are detailed in the Appendix A). They determined, the likelihood of risk occurrence for each risk according to the criteria on the Table 4.4. and the total value of business effect according to the criteria on the Table 4.5.

Then the total risk score was calculated for each risk with regard to the Formula (4.1).

$$\begin{aligned} Total\ Risk\ Score \\ &= Asset\ (Replacement)\ Value\ Rating \\ &\times \big[Likelihood\ of\ Risk\ Occurrence\ Rating \\ &\times \big((Confidentiality\ + Integrity \\ &+ Availability) Business\ Impact\ Rating\big)\big] \end{aligned} \tag{3.1}$$

90 of the 122 risks were scored below 26, 25 risks were scored between 27-71, and 7 risks were scored between 72-135.

5.4. RISK ASSESSMENT

After information security team performed risk analysis and stated the risk scores for each asset, information security executive board carried out Risk Assessment process by following the steps shown in the Figure 4.5.

As a result of risk assessment process 90 risks were rated as low level, 25 risks were rated as medium level and 7 risks were rated as high level according to Risk Level Matrix (Table 4.6).

Table 5.5. Summary table of risks.

Risk Level	Number of Detected Risks
High	7
Medium	25
Low	90
Total	122

Table 5.5 refers to the distribution of detected risks according to their levels. These risks are detailed in the Appendix A.

Information security executive board added explanation concerning why they assigned those risk levels to the relevant risks on the Table 4.3 (See: Appendix A). They also stated the rules for the actions to be taken for each level of risk as shown in the Table 4.7.

5.5. RISK TREATMENT

Information security team decided on the risk treatment methods based on the risk levels of each asset and related action alternatives stated in Table 4.8. Consequently, they decided on risk acceptance method for 82 low level risks, risk monitoring method for 18 medium level risks, risk transfer method for 2 low level risks, 1 medium level risk, and project for 6 low level risks, 6 medium level risks, 7 high level risks.

Table 5.6. Summary table of risk treatment methods based on risk levels.

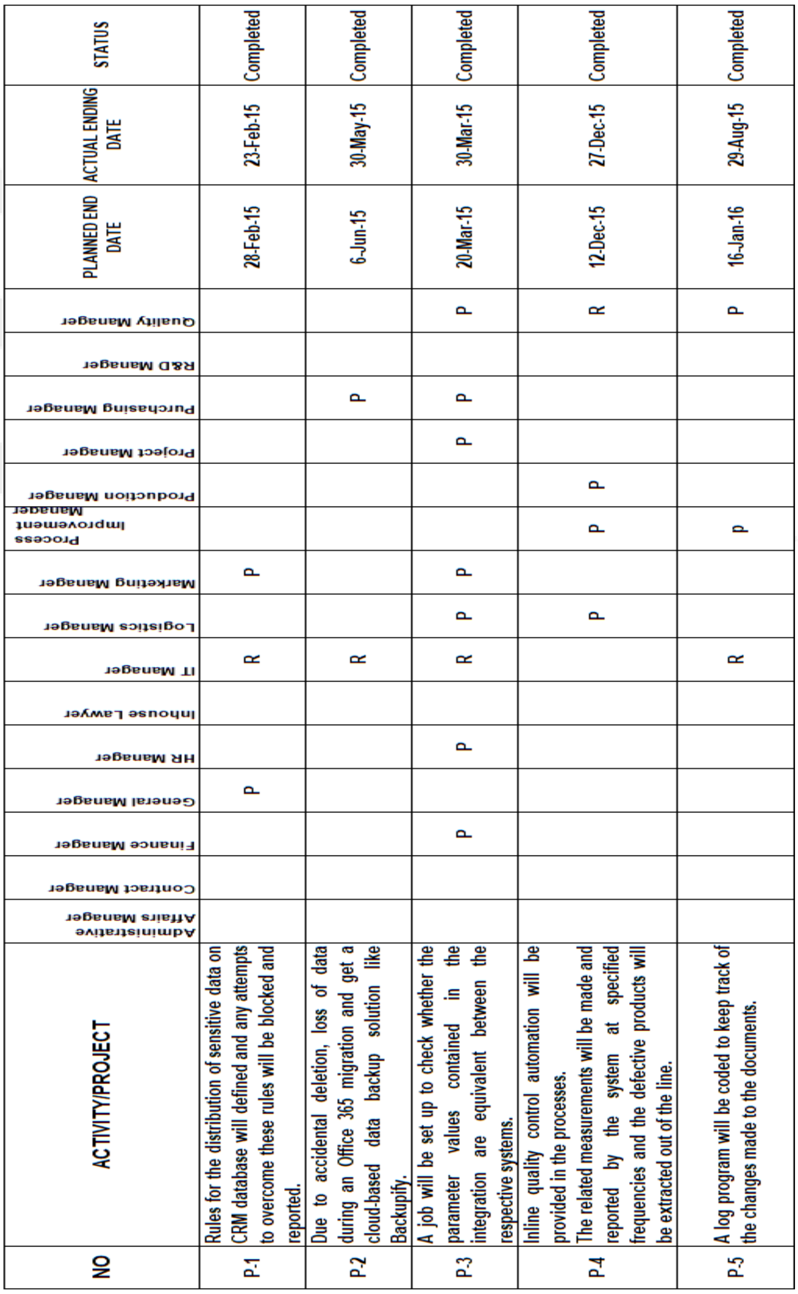
	Risk Level			Total Number of Risks
Risk Treatment Method	Low	Medium	High	
Risk Acceptance	82	x	x	82
Risk Monitoring	x	18	x	18
Risk Transfer	2	1	x	3
Project	6	6	7	19
Grand Total				122

Table 5.6 shows the distribution of chosen risk treatment methods based on the risk level. The chosen risk treatment method for each risk can be seen in the Appendix A.

Then, an action list was prepared regarding to determined risk treatment method for each risk. After each action was completed, risk analysis was repeated, new risk score was re-calculated for the related risk and entered to the “After the Measures Are Taken” part of the Table 4.3. (Actions taken and re-calculated risk score for each risk can be seen in the Appendix A).

Detected high level risks are usually related to business continuity. For example in this study one of the high level risks is business interruption because of natural disasters. Due to natural disasters servers may be damaged and cause business interruption. This risk’s level was asessed as high, so it required to implement a project in order to decrease its level. We established a backup center with stand-by servers in Konya, so if there is an interruption this back-up server will be activated and ensure the business continuity.

Table 5.7. Actions planning table.



NO	ACTIVITY/PROJECT	Administrative Affairs Manager	Contract Manager	Finance Manager	General Manager	HR Manager	Inhouse Lawyer	IT Manager	Logistics Manager	Marketing Manager	Process Improvement Manager	Production Manager	Project Manager	Purchasing Manager	R&D Manager	Quality Manager	PLANNED END DATE	ACTUAL ENDING DATE	STATUS
P-1	Rules for the distribution of sensitive data on CRM database will defined and any attempts to overcome these rules will be blocked and reported.				P			R		P							28-Feb-15	23-Feb-15	Completed
P-2	Due to accidental deletion, loss of data during an Office 365 migration and get a cloud-based data backup solution like Backupify.							R						P			6-Jun-15	30-May-15	Completed
P-3	A job will be set up to check whether the parameter values contained in the integration are equivalent between the respective systems.			P		P		R	P	P			P	P		P	20-Mar-15	30-Mar-15	Completed
P-4	Inline quality control automation will be provided in the processes. The related measurements will be made and reported by the system at specified frequencies and the defective products will be extracted out of the line.								P		P	P				R	12-Dec-15	27-Dec-15	Completed
P-5	A log program will be coded to keep track of the changes made to the documents.							R			p					P	16-Jan-16	29-Aug-15	Completed

The Table 5.7 is the short version of action plan based on the identified risks during risk analysis study, full version is in the Appendix J.

Subsequently, after all actions were taken information security executive board decided that related risks were mitigated and all of them were assigned as low level.

Table 5.8. Summary table of risk treatment methods after projects and actions.

	Risk Level			Total Number of Risks
Risk Treatment Method	Low	Medium	High	
Risk Acceptance	101	x	x	101
Risk Monitoring	x	18	x	18
Risk Transfer	2	1	x	3
Project	x	x	x	x
Grand Total				122

The Table 5.8 shows the distribution of risks and risk treatment methods after projects implementations and taken actions.

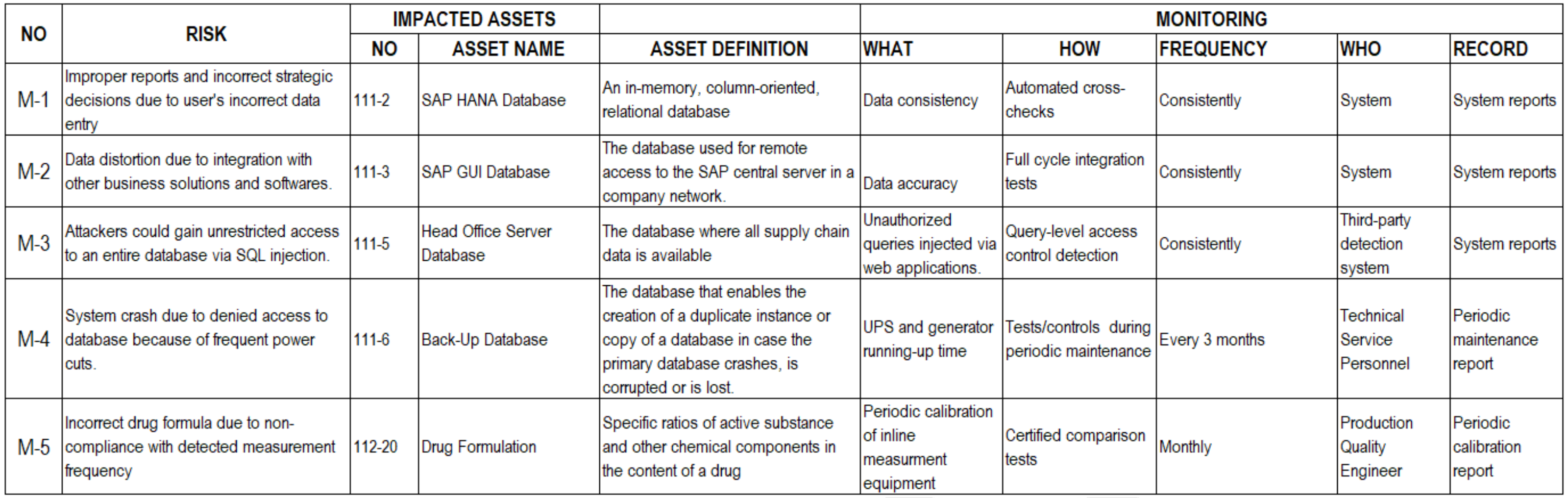
And also we prepared control monitoring plan for all risks to maintain our ISMS system.

5.6. MONITORING THE EFFECTIVENESS OF CONTROLS

Monitoring the effectiveness of controls process was carried out by following the steps shown in the Figure 4.8.

In this study information security team determined controls for 18 risks and prepared the Control Efficiency Monitoring Plan by using the Table 4.9.

Table 5.9. Control efficiency monitoring plan.



NO	RISK	IMPACTED ASSETS			MONITORING				
		NO	ASSET NAME	ASSET DEFINITION	WHAT	HOW	FREQUENCY	WHO	RECORD
M-1	Improper reports and incorrect strategic decisions due to user's incorrect data entry	111-2	SAP HANA Database	An in-memory, column-oriented, relational database	Data consistency	Automated cross-checks	Consistently	System	System reports
M-2	Data distortion due to integration with other business solutions and softwares.	111-3	SAP GUI Database	The database used for remote access to the SAP central server in a company network.	Data accuracy	Full cycle integration tests	Consistently	System	System reports
M-3	Attackers could gain unrestricted access to an entire database via SQL injection.	111-5	Head Office Server Database	The database where all supply chain data is available	Unauthorized queries injected via web applications.	Query-level access control detection	Consistently	Third-party detection system	System reports
M-4	System crash due to denied access to database because of frequent power cuts.	111-6	Back-Up Database	The database that enables the creation of a duplicate instance or copy of a database in case the primary database crashes, is corrupted or is lost.	UPS and generator running-up time	Tests/controls during periodic maintenance	Every 3 months	Technical Service Personnel	Periodic maintenance report
M-5	Incorrect drug formula due to non-compliance with detected measurement frequency	112-20	Drug Formulation	Specific ratios of active substance and other chemical components in the content of a drug	Periodic calibration of inline measurment equipment	Certified comparison tests	Monthly	Production Quality Engineer	Periodic calibration report

The Table 5.9 is the short version of control efficiency monitoring plan of related risks, full version is in the Appendix B.

Over a period of one year, controls that carried out, continuously or periodically, shew that there was no deviation from the required information security conditions.

5.7. MANAGEMENT OF INFORMATION SECURITY EVENTS/BREACHES

Management of information security events/breaches process was carried out by following the steps shown in the Figure 4.9. This process is also in the similar approach as described in Scarfone et al.'s [29] study.

Over a period of one year, 1 information security event and 2 information security breaches were reported. The security event was related to getting a new software for documentation. In order to ensure that required security conditions were met for the related software, information security board carried out a risk analysis. The perceived risk was that an unauthorized person might access confidential data stored in this software. In this respect, access rights were defined in accordance with the responsibilities of employees [19, 20]. Both of the reported information security breaches were cyber attacks. Due to cyber attack detection systems the attacks were repulsed.

5.8. MANAGEMENT REVIEW OF ISMS

Management review of ISMS process was carried out by following the steps shown in the Figure 4.10.

We confirmed that our ISMS system was operating effectively in the Management Review of ISMS meeting held at the end of the year.

6. CONCLUSION

The aim of this study was to develop a methodological framework based on the ISO 27001:2005 standard [5]. As mentioned earlier, this standard just provides a baseline for ISMS implementation, but it does not describe how to conduct the ISMS processes. In order to fill this deficiency, we developed a comprehensive framework, designed process maps describing clearly how to carry out each ISMS operation effectively.

The methodology we proposed is for pharmaceutical industry but it can be used to guide ISMS implementation to different sectors as well.

We performed ISMS implementation at ABC Pharma Solutions in accordance with the developed framework and process maps. Based on the results of our risk analysis study we detected 90 low level risks, 25 medium level risks and 7 high level risks. We implemented 15 projects and took 2 actions in order to mitigate their level. As part of the Risk Treatment process a project should be implemented for all kinds of risks in order to mitigate their level, but due to high level risks are unacceptable, projects must be implemented for high level risks to decrease their level to low or medium level.

In order to use our resources effectively and to keep our costs under control, we implemented projects for limited number of risks. At the end of project implementations and actions taken, level of 7 high risks were reduced to low level and level of 6 medium risks were reduced to low level as well.

Finally, we received the certification by meeting the ISO 27001 requirements. As an ISO 27001 certified company, ABC Pharma Solutions gained competitive advantage and increased the customer portfolio considerably just in 2 years. Additionally, as an FDA approved company we introduced our methodology in a 3 day workshop to be applied in a subsidiary food company in Georgia.

In the growing field of information technology services, information security receives a special attention. Variety of industries and companies support the developments in 27001, thus information security in terms of technology transfer, communication, education and testing. Pharmaceutical industry may be leading the initiatives, but there is no question that other industries will soon be a bigger players in this field.

The methodology we proposed was used for pharmaceutical industry, but it can be used to guide ISMS implementation to different sectors as well. Thus, one of the study’s contributions is that it begins to define in detail how information risk management is carried out in one field and provide framework so that it can be spread to other fields.

REFERENCES

1. Dodge JrRC, Carver C, Ferguson AJ. Phishing for User Security Awareness. *Computers and Security*. 2007; 26(1): 73-80.

2. Posthumus S, Von Solms RA. Framework for the Governance of Information Security. *Computers and Security.* 2004; 23(8): 638-646.

3. Whitman ME, Mattord HJ. *Principles of Information Security*. Boston:Cengage Learning; 2012.

4. Grobler T, Louwrens B. Digital Forensic Readiness as a Component of Information Security Best Practice. *IFIP International Federation for Information Processing.* 2007; 232(9): 13-24.

5. International Organization for Standardization (ISO) and The International Electrotechnical Commission (IEC). ISO/IEC 27001:2005. Information Technology Security Techniques Information Security Management Systems Requirements. Geneva: ISO; 2005.

6. Humphreys L. Mobile Social Networks and Social Practice: A Case Study of Dodgeball. *Journal of Computer-Mediated Communication.* 2007; 13(1): 341-360.

7. Backhouse J, Hsu CW, Silva L. Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard. *MIS Quarterly*. 2006; 30(1): 413-439.

8. Calder A, Watkins SG. *Information Security Risk Management for ISO27001/ISO27002.* Cambridgeshire: It Governance; 2007.

9. Thomas G, Botha RA. Secure Mobile Device Use in Healthcare Guidance from HIPAA and ISO17799. *Information Systems Management*. 2007; 24(4): 333-342.

10. Rowlingson R, Winsborrow R. A. Comparison of the Payment Card Industry Data Security Standard with ISO17799. *Computer Fraud and Security*. 2006; 2006(3): 16-19.

11. Cyber and Insider Risk at a Glance: The Pharmaceutical Industry; [cited 2018 3 October]. Available from: https://www2.deloitte.com/content/dam/Deloitte/jp /Documents/life-sciences-health-care/ls/jp-ls-cyber-insider-risk-en.pdf.

12. Brenner J. ISO 27001: Risk Management and Compliance. *Risk Management Magazine*. 2007; 54(1): 24-29.

13. Hazari S. Perceptions of End-Users on The Requirements in Personal Firewall Software: An Exploratory Study; [cited 2019 7 May]. Available From: https:// www. sunilhazari.com/education/documents1/articles/Hazari_Firewall.pdf.

14. Von Solms R. Information Security Management (3): The Code of Practice for Information Security Management (BS 7799). *Information Management and Computer Security*. 1998; 6(5): 224-225.

15. Ma Q, Johnston AC, Pearson JM. Information Security Management Objectives and Practises: A Parsimonious Framework. *Information Management and Computer Security*. 2008; 16(3): 251-270.

16. Siponen M, Baskerville R, Heikka JA. Design Theory for Secure Information Systems Design Methods. *Journal of the Association for Information Systems*. 2006; 7(1): 31.

17. Bulgurcu B, Cavusoğlu H, Benbasat I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*. 2010; 34(3): 523-548.

18. Safa NS, Soms RV, Furnell S. Information Security Policy Compliance Model in Organizations. *Computers and Security*.2015; 56(C): 1-13.

19. Lee J, Lee Y. A Holistic Model of Computer Abuse within Organizations. *Information Management and Computer Security*. 2002; 10(2): 57-63.

20. Straub JrDW, Nance WD. Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly*.1990; 14(1): 45-60.

21. Chen PS, Yen DC, Lin SC. The Classification of Information Assets and Risk Assessment: An Exploratory Study Using the Case of C-Bank. *Journal of Global Information Management.* 2015; 23(4): 1-29.

22. Park CS, Jang SS, Park YT. A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance. *IJCSNS International Journal of Computer Science and Network Security*. 2010; 10(3): 10-21.

23. Berström E, Ahlfeldt RM. Information Classification Issues; [cited 2019 21 March]. Available from:https://link.springer.com/chapter/10.1007%2F978-3-319-11599-3_2.

24. Blakley B, McDermott E. Information Security is Information Risk Management. *Nspw01 Proceedings of the 2001 Workshop on New Security Paradigms*. 2001: 97-104.

25. Rainer KR, Snyder CA, Carr AH. Risk Analysis for Information Technology. *Journal of Management Information Systems.* 1991; 8(1): 29-64.

26. Amancei C. Practical Methods for Information Security Risk Management. *Informatica Economică.* 2011; 15(1): 151-159.

27. Seale M. Risk Register and Risk Treatment Plan [cited 2019 10 January]. Available from:https://isoconsultantpune.com/wp-content/uploads/2017/03/risk-treatment-plan.pdf

28. Humberto M, Pelaez S. Measuring Effectiveness in Information Security Controls [cited 2018 24 March]. Available from: https: //www.sans.org/readingroom/ whitepapers /basics/paper/33398.

29. Scarfone K, Cichonski P, Millar T, Grance T. Computer Security Incident Handling Guide. NIST Special Publication [cited 2017 17 April]. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

30. Kosutic D. The ISO 27001 and ISO 22301 Blog; [cited 2019 17 April]. Available from: https://advisera.com/27001academy/blog/2014/03/03/why-is-management-review-important-for-ISO-27001-and-ISO-22301.

APPENDIX A: RISK ANALYSIS

Table A.1. Risk analysis.

BEFORE MEASURES																	AFTER MEASURES											
						BUSINESS IMPACT			TOTAL										BUSINESS IMPACT			TOTAL					
RISK NO	ASSET ID	ASSET	RISKS	REPLACEMENT VALUE	LIKELIHOOD of RISK OCCURRENCE	CONFIENDIALITY	INTEGRITY	AVAILABILITY	CONFIENDIALITY	INTEGRITY	AVAILABILITY	TOTAL RISK SCORE	RISK LEVEL	EXPLANATION	RISK TREATMENT METHOD	PROJECT/ MONITORING NO	REPLACEMENT VALUE	LIKELIHOOD of RISK OCCURRENCE	CONFIENDIALITY	INTEGRITY	AVAILABILITY	CONFIENDIALITY	INTEGRITY	AVAILABILITY	RESIDUAL RISK SCORE	RISK LEVEL	STATUS
1	111-1	CRM Database	Loss of customers as a result of employees passing the customer information intentionally or unintentionally into the hands of competitors.	3	4	3	1	1	12	4	4	60	MEDIUM	Although certain individuals were granted access to the data, a monitoring system was not available.	PROJECT	P-1	3	1	3	1	1	3	1	1	15	ACCEPTABLE RISK	CLOSED
2	111-2	SAP HANA Database	Improper reports and incorrect strategic decisions due to user's incorrect data entry	3	2	1	3	1	2	6	2	30	MEDIUM	Automated cross-checks are available at every step throughout the data entry process.	MONITORING	M-1	3		1	3	1	0	0	0	0	ACCEPTABLE RISK	CLOSED
3	111-3	SAP GUI Database	Data distortion due to integration with other business solutions and softwares.	3	2	1	3	1	2	6	2	30	MEDIUM	Full cycle integration tests are performed.	MONITORING	M-2	3		1	3	1	0	0	0	0	ACCEPTABLE RISK	CLOSED

4	**111-4**	Web Database	Malicious attack via a request sent from a third-party web site in order to access functionality of a victim's authenticated browser.	**3**	**2**	**1**	**2**	**1**	**1**	**1**	**2**	**24**	**LOW**	There is an automated scanning and auditing mechanism which monitors for malicious attempt.	**RISK ACCEPTENCE**	**-**		**3**		**1**	**2**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
5	**111-5**	Head Office Server Database	Attackers could gain unrestricted access to an entire database via SQL injection.	**3**	**2**	**3**	**2**	**2**	**6**	**4**	**4**	**42**	**MEDIUM**	Query-level access control detects unauthorized queries injected via web applications.	**MONITORING**	**M-3**		**3**		**3**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
6	**111-6**	Back-Up Database	System crash due to denied access to database because of frequent power cuts.	**3**	**2**	**1**	**3**	**3**	**2**	**6**	**6**	**42**	**MEDIUM**	In case of an power cut, there is a UPS and generator that will meet the need for energy during 24 hours.	**MONITORING**	**M-4**		**3**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
7	**112-1**	Quality Management Systems Documents	Deletion / disappearance of documents due to a technical problem	**2**	**5**	**2**	**3**	**3**	**10**	**15**	**15**	**80**	**HIGH**	Documents are kept on the fileserver and backups are taken every day.	**PROJECT**	**P-2**		**2**	**1**	**2**	**3**	**3**	**2**	**3**	**3**	**16**	**ACCEPTABLE RISK**	**CLOSED**
8	**112-2**	Information Security Management Documents	Information security breaches due to lack of updating documents according to information security rules.	**2**	**2**	**1**	**3**	**1**	**2**	**6**	**2**	**20**	**LOW**	Periodic reviews are made for the need for updating in the documentation. When there is a change in the legislation, instant updates are made based on information from official channels.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**3**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
9	**112-3**	Information Security Risk Management Records	Error retrieving information security violation records, due to the failure of integration among different systems,	**2**	**5**	**3**	**3**	**3**	**15**	**15**	**15**	**90**	**HIGH**	There are 5 separate systems integration and complicated user interfaces, therefore likelihood of occurrence is very high.	**PROJECT**	**P-3**		**2**	**1**	**3**	**3**	**3**	**3**	**3**	**3**	**18**	**ACCEPTABLE RISK**	**CLOSED**
10	**112-4**	Nonconformity Records	Due to lack of communication missing nonconformity records, customer unsatisfaction.	**2**	**2**	**1**	**2**	**1**	**2**	**4**	**2**	**16**	**LOW**	Records are kept by Quality Systems Engineer and compared with e-mails.	**RISK ACCEPTENCE**	**-**												

11	**112-5**	Calibration Records	Because the periodic calibrations of equipments are not cınducted, defected products maybe sent to customers.	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**6**	**LOW**	Periodic maintenance of the equipment which are subject to calibration is done by an external firm and calibrations are made before the expiry date. A list of devices subject to calibration has been created. Periodically reviewed.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
12	**112-6**	Project Records	Loss of project records due to the intranet system crash for any reason.	**2**	**2**	**1**	**2**	**3**	**2**	**4**	**6**	**24**	**LOW**	Project records are also kept in the fileserver and backups are taken.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
13	**112-7**	Quality Control Records	Delivery of defective products due to failure to comply with the specified measurement frequency	**2**	**2**	**0**	**0**	**3**	**0**	**0**	**6**	**12**	**LOW**	The records are periodically monitored by Quality Systems Engineer within the framework of QC plan.	**PROJECT**	**P-4**		**2**	**1**	**0**	**0**	**3**	**0**	**0**	**3**	**6**	**ACCEPTABLE RISK**	**CLOSED**
14	**112-8**	Corporate Performance Management Records	Uncontrolled changes by unauthorized persons in existing documents	**2**	**4**	**1**	**3**	**1**	**4**	**12**	**4**	**40**	**MEDIUM**	An access authorization policy is available, only authorized personnel can do changes in documents which they are responsible for.	**PROJECT**	**P-5**		**2**	**2**	**1**	**3**	**1**	**2**	**6**	**2**	**20**	**ACCEPTABLE RISK**	**CLOSED**
15	**112-9**	Payroll Information	Access to payroll information by unauthorised persons and decreas in employee motivation	**2**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**20**	**LOW**	The payroll data is available on the SAP HR module. It it is only accessible by Hr Manager and Payroll& Benefits Specialist. Log report of who accessed the relevant data is shared with IT Manager.	**RISK ACCEPTENCE**	**-**		**2**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
16	**112-10**	Business Contracts	Breach of contract as a result of not keeping a record of the revisions in the contract due to lack of staff responsible for work contracts	**2**	**2**	**1**	**2**	**2**	**2**	**4**	**4**	**20**	**LOW**	Purchasing department carries out contract management activities.	**PROJECT**	**P-6**		**2**	**1**	**1**	**2**	**2**	**1**	**2**	**2**	**10**	**ACCEPTABLE RISK**	**CLOSED**

17	**112-11**	Personnel Affairs Documents	Inconsistency among the amounts of wage in candidates offer letters, employment contracts and accounting records.	**2**	**2**	**1**	**3**	**1**	**2**	**6**	**2**	**20**	**LOW**	In case of inconsistency, the amount on the wet signed contract is considered data.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**3**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
18	**112-12**	IT Equipment Records	Failure to make accurate backup plan because the information of IT equipment locations are not updated in the inventory list in case of any physical transfer.	**1**	**2**	**0**	**1**	**3**	**0**	**2**	**6**	**8**	**LOW**	Inventory counts are made periodically and information is updated in the list.	**PROJECT**	**P-7**		**1**	**1**	**0**	**1**	**3**	**0**	**1**	**3**	**4**	**ACCEPTABLE RISK**	**CLOSED**
19	**112-13**	Proxy Permission List	Unauthorized access to a secret information due to error in access authorization process.	**1**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**10**	**LOW**	Access to all persons is determined and controlled according to a specific approval mechanism in the access rights matrix.	**RISK ACCEPTENCE**	**-**		**1**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
20	**112-14**	Health Ministry Correspondence Files	Changes on documents by unauthorized personnel	**1**	**2**	**3**	**2**	**1**	**6**	**4**	**2**	**12**	**LOW**	Overwriting, reading and deleting rights are defined and all changes on the document is logged.	**RISK ACCEPTENCE**	**-**		**1**		**3**	**2**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
21	**112-15**	Customer Information	Access to customer information by unauthorised persons and loss of competitive power.	**3**	**5**	**3**	**1**	**1**	**15**	**5**	**5**	**75**	**HIGH**	Customer information can be accessed as a whole, there is no information encryption according to the relevant position	**PROJECT**	**P-8**		**3**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**15**	**ACCEPTABLE RISK**	**CLOSED**
22	**112-16**	Approved Vendor List	Unauthorized drug distribution to pharmacies due to not checking the Ministry of Health approval certificate.	**2**	**3**	**3**	**1**	**1**	**9**	**3**	**3**	**30**	**MEDIUM**	Ministry of Health approvals are checked manually, there is no system integration.	**PROJECT**	**P-9**		**2**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**10**	**ACCEPTABLE RISK**	**CLOSED**
23	**112-17**	Vendor Information	Sharing the offer files of the vendors with non-related people.	**2**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**20**	**LOW**	Offer files of vendors are only shared with the purchasing manager.	**RISK ACCEPTENCE**	**-**		**2**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
24	**112-18**	Financial Statements	Error in financial reports after incorrect data entry and accordingly making strategic decisions incorrectly	**2**	**2**	**2**	**1**	**2**	**4**	**2**	**4**	**20**	**LOW**	The data entered into the system are recorded with the approval of the financial manager.	**RISK ACCEPTENCE**	**-**		**2**		**2**	**1**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

25	**112-19**	Formal Reports	Due to lack of registration of revisions to the formal reportz, analysis cannot be performed.	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**8**	**LOW**	The actuality of the report contents is periodically checked by the unit manager	**RISK ACCEPTENCE**	**-**		**2**		**1**	**2**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
26	**112-20**	Drug Formulation	Incorrect drug formula due to non-compliance with detected measurement frequency	**3**	**2**	**1**	**3**	**1**	**2**	**6**	**2**	**30**	**MEDIUM**	Inline measurement automation available. Measurement equipment's periodic calibration is provided.	**MONITORING**	**M -5**		**3**		**1**	**3**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
27	**112-21**	Production Reports	Incorrect reporting due to error during manual data entry	**1**	**2**	**1**	**3**	**1**	**2**	**6**	**2**	**10**	**LOW**	A second control is provided after data entries, the likelihood of occurrence is low	**RISK ACCEPTENCE**	**-**		**1**		**1**	**3**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
28	**112-22**	Machine Information and Instructions for Use	Machine faults, quality problems after incorrect use due to incomplete / out-of-machine instructions	**1**	**2**	**1**	**2**	**2**	**2**	**4**	**4**	**10**	**LOW**	Machine maintainance manager is responsible for updating machine instructions due to changes.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
29	**112-23**	Change Request Records	Disruptions as a result of not carrying out impact analyzes of changes in processes related to each other	**1**	**3**	**2**	**2**	**3**	**6**	**6**	**9**	**21**	**LOW**	Change management procedure is executed and changes are made via CR form	**RISK ACCEPTENCE**	**-**		**1**		**2**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
30	**112-24**	Inventory Information	Incorrect detection of inventory amount as a result of error in manual entry of goods receiving and goods issue processes.	**1**	**5**	**1**	**3**	**3**	**5**	**15**	**15**	**35**	**MEDIUM**	There is high likelihood of errors in manual inventory quantities entry.	**PROJECT**	**P-10**		**1**	**2**	**1**	**3**	**3**	**2**	**6**	**6**	**14**	**ACCEPTABLE RISK**	**CLOSED**
31	**112-25**	Shipment Reports	Manipulation of data on delayed shipments in the report, customer complaints	**1**	**1**	**3**	**2**	**2**	**3**	**2**	**2**	**7**	**LOW**	Due to shipment reports are generated as pdf reports, the real data can not be changed.	**RISK ACCEPTENCE**	**-**		**1**		**3**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
32	**112-26**	Operational Dashboard	Due to incorrect data entry, wrong strategic decisions and actions.	**1**	**3**	**2**	**3**	**2**	**6**	**9**	**6**	**21**	**LOW**	There are cross-checks on each step during the reporting process.	**RISK ACCEPTENCE**	**-**		**1**		**2**	**3**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
33	**112-27**	All Data Files on File Server	Data loss due to problems in disks.	**3**	**2**	**1**	**2**	**3**	**2**	**4**	**6**	**36**	**MEDIUM**	Likelihood of occurrence is low,because the San unit is tolerated up to 3 discs and is controlled every day.	**MONITORING**	**M -6**		**3**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

34	**112-28**	All Data Files on Sharepoint	Data loss due to failure of the backup system.	**3**	**1**	**1**	**2**	**3**	**1**	**2**	**3**	**18**	**LOW**	There has been no loss in the past. When the backup cannot be done, a warning e-mail is received.	**RISK ACCEPTENCE**	**-**		**3**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
35	**112-29**	Camera Records	Failure to register as a result of not starting the camera program at the end of working hours due to the office assistant's absence.	**2**	**3**	**2**	**2**	**2**	**6**	**6**	**6**	**36**	**MEDIUM**	It is stated in the deputation matrix that the security officer will undertake this task in case of office assistant's absence..	**MONITORING**	**M-7**		**2**		**2**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
36	**113-1**	ISO 9001 Quality Documents	Deletion / disappearance of documents due to a technical problem	**1**	**2**	**1**	**3**	**3**	**2**	**6**	**6**	**14**	**LOW**	Each document created in the document management system QDMS is simultaneously copied in the cloud.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
37	**113-2**	Invoices	Recurring e-invoices due to coding error	**1**	**2**	**2**	**3**	**3**	**4**	**6**	**6**	**16**	**LOW**	Crontab job does not allow the system to interrupt the recurring invoice.	**RISK ACCEPTENCE**	**-**		**1**		**2**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
38	**221-1**	Notebooks	Security openings due to failure of the operating system updates and consequently hacker attacks	**2**	**3**	**3**	**1**	**1**	**9**	**3**	**3**	**30**	**MEDIUM**	Operating Systems updates are done automatically.	**MONITORING**	**M-8**		**2**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
39	**221-2**	Printers	A secret document may be printed out and forgetten. And an unauthorized person may got and disclose it.	**2**	**5**	**3**	**1**	**1**	**15**	**5**	**5**	**50**	**MEDIUM**	Due to lack of control, likelihood of occurrence is high.	**PROJECT**	**P-11**		**2**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**10**	**ACCEPTABLE RISK**	**CLOSED**
40	**221-3**	Head Office Servers	The loss of data within our servers as a result of flooding and our system will not work for a certain period of time	**3**	**2**	**1**	**1**	**3**	**2**	**2**	**6**	**30**	**MEDIUM**	With the scheduled task, the health of raid filesystem server disks is controlled.	**MONITORING**	**M-9**		**3**		**1**	**1**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
41	**221-4**	Web App Server	Servers overheating due to failure of the air conditioner and temperature values can not be controlled	**3**	**2**	**1**	**3**	**3**	**2**	**6**	**6**	**42**	**MEDIUM**	To ensure optimum operation of the servers, a 3-way cooling system has been installed and the task is controlled to send e-mails to the relevant personnel when the task exceeds 24 C.	**MONITORING**	**M-10**		**3**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

42	**221-5**	Backup Database Server	Unauthorized personnel entry into the server room or an attempt to be entered forcibly due to a data privacy violation and data theft.	**3**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**30**	**MEDIUM**	The server room is protected by security guards of the entrance of the building where the only card access to the building can be made, the server repeatedly to the entrance to the room is physically secured the adoption of encrypted 2 door and followed with instant cameras.	**MONITORING**	**M-11**		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
43	**221-6**	BPC Database Server	Servers maybe damaged by sudden voltage changes due to frequent power outages	**3**	**1**	**1**	**1**	**3**	**1**	**1**	**3**	**15**	**LOW**	In case of power failure UPS is in operation, 24 hours a day with sufficient capacity generator available.	**RISK ACCEPTENCE**	**-**		**3**		**1**	**1**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
44	**221-7**	CRM Database Server	Fire outbreak in server room.	**3**	**1**	**1**	**3**	**3**	**1**	**3**	**3**	**21**	**LOW**	The FM200 fire extinguisher system was installed and activated in order to detect a fire in the event of a fire.	**RISK ACCEPTENCE**	**-**		**3**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
45	**221-8**	SAP Applications Server	Crash of servers as a result of earthquakes	**3**	**4**	**1**	**3**	**3**	**4**	**12**	**12**	**84**	**HIGH**	In order to prevent data loss in natural disasters of the data, a steel safe was taken. In order not to lose our data and to keep our system working, we will work in a redundant manner with the current server and necessary equipment will be installed.	**PROJECT**	**P-12**		**3**	**1**	**1**	**3**	**3**	**1**	**3**	**3**	**21**	**ACCEPTABLE RISK**	**CLOSED**
46	**222-1**	Mobile Phones	In case of theft of mobile phones, secret company information may be disclosed by an unauthorized person because the device doesn't require the password.	**2**	**2**	**3**	**1**	**2**	**6**	**2**	**4**	**24**	**LOW**	The company phones have a password rule via MDM, and after 15 seconds, the phones go to sleep mode.	**RISK ACCEPTENCE**	**-**		**2**		**3**	**1**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
47	**222-3**	IP Telephones	In case of internet cut, telephone line does not work, and customer may not reach by phone.	**1**	**3**	**1**	**3**	**3**	**3**	**9**	**9**	**21**	**LOW**	Since there is a possibility of working with mobile internet line, mobile line is activated in case of an interruption in fixed internet line.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
48	**223-1**	Backup Cartridges	Failure to retrieve backups due to inadequate backup system	**3**	**2**	**2**	**2**	**3**	**4**	**4**	**6**	**42**	**MEDIUM**	If there is a problem in the backup process, the backup system occupancy rate is increasing. The occupancy rate of the backup area is reported to the alert e-mail alarm system.	**MONITORING**	**M-12**		**3**		**2**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

49	**223-2**	CCTV Server	Loss of camera records due to inaccurate assembling of the equipments. Failure to follow a possible theft.	**2**	**2**	**3**	**3**		**6**	**6**	**0**	**24**	**LOW**	Tests are carried out after the camera installation and the correct recording is confirmed.	**RISK ACCEPTENCE**	**-**		**2**		**3**	**3**	**0**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
50	**223-3**	Portable Hard Drives	Due to software malfunction, the logs can not be erased. Backups may not be taken becuase of the full memory.	**2**	**2**	**2**	**3**	**3**	**4**	**6**	**6**	**32**	**MEDIUM**	If there is a problem in the backup process, the backup system occupancy rate is increasing. The occupancy rate of the backup area is reported to the alert e-mail alarm system.	**MONITORING**	**M - 13**		**2**		**2**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
51	**223-4**	SSD	Hackers may access to information on the SSD, because the firewall is exceeded.	**3**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**15**	**LOW**	SSDs are encrypted and cannot be accessed except authorized person.	**RISK ACCEPTENCE**	**-**		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
52	**224-1**	Firewall Machine	Because of configuration mistakes hackers may access the company information.	**3**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**15**	**LOW**	Firewall Manager is used, it ensure existing and newly created resources comply with a mandatory set of security policies automatically and configures the firewall properly.	**RISK ACCEPTENCE**	**-**		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
53	**224-2**	Accesspoints	Internet connection may not be provided in some areas, because the access points are not installed according to stated layout.	**1**	**1**	**1**	**3**	**3**	**1**	**3**	**3**	**7**	**LOW**	The AP installations are carried out by the contractor firm and it is confirmed by the administrative affairs department that the installation is done in a compliance with our layout.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
54	**224-3**	Routers	Due to weak password hackers may access usernames,sensitive company information, emails, and more flowing through an encrypted WiFi network.	**2**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**10**	**LOW**	Complex password policy is available.	**RISK ACCEPTENCE**	**-**		**2**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
55	**224-4**	VPN Appliance	Attackers may get their identity information authorized with the help of spoofing through emails or Ips	**2**	**3**	**3**	**1**	**1**	**9**	**3**	**3**	**30**	**MEDIUM**	Identification authenticatication is based on keys which are shared between the client and server.	**MONITORING**	**M - 14**		**2**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

56	**224-5**	Switches	Deletion of the configuration on the backbone switch due to a power cut and consequently the lack of internet connection.	**1**	**3**	**2**	**2**	**3**	**6**	**6**	**9**	**21**	**LOW**	In case of an power cut, there is a UPS and generator that will meet the need for energy during 24 hours.	**RISK ACCEPTENCE**	**-**		**1**		**2**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
57	**224-6**	Gateways	Interruption of communication of 2 separate networks within the company as a result of failure of Gateway settings	**2**	**3**	**1**	**1**	**2**	**3**	**3**	**6**	**24**	**LOW**	In such a case, the IT department can quickly make the necessary adjustments.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**1**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
58	**225-1**	Barcode Readers	Goods issue may not be recorded on the system due to interruption of wifi connection. Consequently, there may be inconsistency between physical stock quantity and system records.	**2**	**2**	**1**	**3**	**2**	**2**	**6**	**4**	**24**	**LOW**	If wifi connection is interrupted, 3g connection is activated automatically immediately.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**3**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
59	**225-2**	Cameras	Unauthorized persons may access to camera records and share process records with competitors.	**2**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**20**	**LOW**	The Camera Access Authorization matrix is available and no-one can access it except authorized people.	**RISK ACCEPTENCE**	**-**		**2**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
60	**225-3**	Raw Materials	A staff may steal company material, because there is no control.	**2**	**2**	**3**	**1**	**2**	**6**	**2**	**4**	**24**	**LOW**	The facility is monitored 7/24, that's why the likelihood of occurrence is low.	**PROJECT**	**P-13**		**2**	**1**	**3**	**1**	**2**	**3**	**1**	**2**	**12**	**ACCEPTABLE RISK**	**CLOSED**
61	**225-4**	Spare Parts	Spare parts maybe damaged during transportation.	**2**	**4**	**1**	**1**	**1**	**4**	**4**	**4**	**24**	**LOW**	Spare parts are insured under the guarantee of the shipping company.	**TRANSFER**	**-**		**2**		**1**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
62	**225-5**	Fire Detection and Alarm System Equipments	Fire due to lack of periodic maintenance of fire-extinguishing system.	**3**	**2**	**1**	**1**	**2**	**2**	**2**	**4**	**24**	**LOW**	A periodic maintenance contract has been made and also insurance is available.	**TRANSFER**	**-**		**3**		**1**	**1**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
63	**225-6**	Finished Products	Outsourced logistics personnel may steal finished products during the loading process.	**3**	**2**	**2**	**1**	**1**	**4**	**2**	**2**	**24**	**LOW**	Loading operations carried out under the supervision of a security officer. The likelihood of occurrence is low.	**RISK ACCEPTENCE**	**-**		**3**		**2**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
64	**225-7**	UPS	Due to sudden high voltage waves, power cut may occur. As a result, systems may not be accessed.	**1**	**1**	**1**	**3**	**3**	**1**	**3**	**3**	**7**	**LOW**	The current coming to the UPS is balanced via regulator.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

65	**225-8**	Entrance Turnstile	An unauthorized person may find a lost security pass and enter the facility.	**3**	**3**	**3**	**2**	**1**	**9**	**6**	**3**	**54**	**MEDIUM**	The staff is responsible for maintaining their card. In case of a loss, he/she informs the IT department, the transition privileges on the card are removed.	**MONITORING**	**M - 15**		**3**		**3**	**2**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
66	**225-9**	Laboratory Equipments	Due to lack of access control to laboratory, equipments and materials may be stolen by unauthorized person.	**3**	**5**	**3**	**2**	**2**	**15**	**10**	**10**	**105**	**HIGH**	Entrance to the lab is done by security pass. However, any person can enter the card of a person with authorization.	**PROJECT**	**P-14**		**3**	**1**	**3**	**2**	**2**	**3**	**2**	**2**	**21**	**ACCEPTABLE RISK**	**CLOSED**
67	**225-10**	Production Machines	Fault in production data due to interruption of SAP system integrated into machines	**3**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**18**	**LOW**	Consistency of production data is ensured during the process, in case of inconsistency machines stop automatically untill data is corrected.	**RISK ACCEPTENCE**	**-**		**3**		**2**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
68	**225-11**	Coding Machines	The production of counterfeit products as a result of the copying of the data matrix loaded into the coding machine.	**3**	**1**	**3**	**2**	**2**	**3**	**2**	**2**	**21**	**LOW**	All data matrices are encrypted.	**RISK ACCEPTENCE**	**-**		**3**		**3**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
69	**331-1**	Windows	Due to physical crashes or some irreverseble disasters corruption of operating system	**2**	**2**	**1**	**2**	**3**	**2**	**4**	**6**	**24**	**LOW**	System Image Backups are available. In case of systems corruption the entire system can be restored.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
70	**331-2**	Android	Collapse ot the android operating system after downloading an application containing virus.	**2**	**2**	**3**	**1**	**2**	**6**	**2**	**4**	**24**	**LOW**	Mobile Device Management is available. IT admins manage permissions requested by mobile apps and give no permission as it can indicate malicious behavior.	**RISK ACCEPTENCE**	**-**		**2**		**3**	**1**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
71	**332-1**	Fiori Mobile	Customers may not use the application due to system work process occupancy.	**2**	**2**	**1**	**1**	**3**	**2**	**2**	**6**	**20**	**LOW**	If customers cannot pass their orders through the application, they are redirected to the website.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**1**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

72	**332-2**	Cryptolog	User A may send a secret file to user B via e-mail. This file may be monitored by another user and copy of this file may be taken by him.	**1**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**5**	**LOW**	Symmetric encryption for large files and Asymmetric Encryption for small messages are available.	**RISK ACCEPTENCE**	**-**		**1**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
73	**332-3**	MS Office Programs	Because there is no restriction of macros, an adversary can create macros to perform a variety malicious activities and deny access to sensitive information.	**2**	**4**	**3**	**1**	**1**	**12**	**4**	**4**	**40**	**MEDIUM**	There is no restriction for macros, and likelihood of occurrence is high.	**PROJECT**	**P-15**		**2**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**20**	**ACCEPTABLE RISK**	**CLOSED**
74	**332-4**	Web Server Software	There may be interruption in the publication of the web site due to bug on Jboss Application server software	**3**	**1**	**1**	**2**	**3**	**1**	**2**	**3**	**18**	**LOW**	Java software is automatically controlled, and an alarm message sent to responsibles in case of any interruption.	**RISK ACCEPTENCE**	**-**		**3**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
75	**332-5**	SAP	Incorrect e-invoicing due to coding error and consequently customer dissatisfaction	**3**	**5**	**2**	**3**	**1**	**10**	**15**	**5**	**90**	**HIGH**	Since there is no invoice simulation program, the probability of occurrence is high.	**PROJECT**	**P-16**		**3**	**1**	**2**	**3**	**1**	**2**	**3**	**1**	**18**	**ACCEPTABLE RISK**	**CLOSED**
76	**332-6**	QDMS	Unauthorized person access to the system, making changes to critical documents.	**1**	**3**	**3**	**2**	**3**	**9**	**6**	**9**	**24**	**LOW**	Access authorization matrix is available and new authorizations are made by administrator approval	**RISK ACCEPTENCE**	**-**		**1**		**3**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
77	**332-7**	Exchange Server	Failure to receive field activation data due to software failure	**1**	**1**	**1**	**2**	**3**	**1**	**2**	**3**	**6**	**LOW**	The software which the field activation systems are connected to is controlled continuously and automatically. An alarm message sent to responsibles in case of any interruption.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
78	**332-8**	TrendMicro	Due to outdated version of antivirus program, viruses may cause data loss.	**3**	**1**	**2**	**2**	**3**	**2**	**2**	**3**	**21**	**LOW**	The actuality of the antivirus system is provided centrally and automatically.	**RISK ACCEPTENCE**	**-**		**3**		**2**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
79	**332-9**	Microsoft Office 365	Due to accidental deletion, loss of data.	**1**	**2**	**1**	**3**	**3**	**2**	**6**	**6**	**14**	**LOW**	Data in use replicated to cloud, in case of data loss it will be available over cloud.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
80	**333-1**	SAP System Software	Production of faulty reports as a result of not running scheduled jobs.	**2**	**2**	**1**	**2**	**3**	**2**	**4**	**6**	**24**	**LOW**	Reporting tools run smoothly with database control panel.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

81	**333-2**	Master PC Systems Software	Due to complicated user interface there may be data lass in the database.	**2**	**2**	**1**	**1**	**3**	**2**	**2**	**6**	**20**	**LOW**	Grid control program automatically controls if the database program runs smoothly. In case of problem, the e-mail alarm message is provided with this GridControl program.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**1**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
82	**333-3**	Back Up Software	Failure of the related job to fail due to system date settings and not receiving reports of serial number of drugs produced	**1**	**2**	**1**	**2**	**3**	**2**	**4**	**6**	**12**	**LOW**	The production stops when the barcode program, in which serial number of the product packages passed through the production line, is not recorded.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
83	**333-4**	Compilers	Sensitive information may be left in the memory because the memory overwritng code is removed by optimizing compiler.	**3**	**4**	**3**	**2**	**2**	**12**	**8**	**8**	**84**	**HIGH**	There is no a control mechanism if overwriting code works or not.	**PROJECT**	**P-17**		**3**	**1**	**3**	**2**	**2**	**3**	**2**	**2**	**21**	**ACCEPTABLE RISK**	**CLOSED**
84	**333-5**	Debuggers	Debugging mode may cause an open port for attackers and they can get full access to system.	**3**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**15**	**LOW**	Debugging mode is disabled and in case of any need security team monitor the system during debugging process	**RISK ACCEPTENCE**	**-**		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
85	**333-6**	Browsers	Phishing attacks, due to malicious pop-up ads,	**3**	**1**	**3**	**2**	**2**	**3**	**2**	**2**	**21**	**LOW**	Browsers are configured to block pop-up ads.	**RISK ACCEPTENCE**	**-**		**3**		**3**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
86	**333-7**	Disk Cleaner	Operating system may not work adequately if there is a lack of free space on the computer's hard disk.	**1**	**2**	**1**	**3**	**3**	**2**	**6**	**6**	**14**	**LOW**	Disk space optimizer tool is used.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
87	**333-8**	Remote Access Software	When log in to e-mail account while using VPN, the e-mail password maybe taken by unauthorized person. He/she may send e-mails on behalf of owner of that adress.	**1**	**3**	**3**	**1**	**1**	**9**	**3**	**3**	**15**	**LOW**	Data confidentiality is provided by ssl encryption method.	**RISK ACCEPTENCE**	**-**		**1**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
88	**441-1**	Customer Support Service	Failure to follow up the service contract due to lack of personnel. hardware-driven interruption as a result of the contract ending, delay of the solution of possible problems	**1**	**1**	**1**	**2**	**2**	**1**	**2**	**2**	**5**	**LOW**	Our service suppliers inform us when it is time to renew the contract, so likelihood of occurrence is low.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

89	**441-2**	SAP Software Maintenance Service	Failure to follow up the service contract due to lack of personnel. Loss of data may occur because of the poor functionality of database.	**2**	**1**	**1**	**2**	**2**	**1**	**2**	**2**	**10**	**LOW**	Our service suppliers inform us when it is time to renew the contract, so likelihood of occurrence is low.	**RISK ACCEPTENCE**	-		**2**		**1**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
90	**441-3**	SAP Licence Maintenance Service	Audit nonconformity due to not following the user licence and using copied licence.	**2**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**20**	**LOW**	Procedure for user registration and de-registration is available. IT responsible gives the licence authority with the approval of their manager. If there is no idle licence, purchase of the new one is provided.	**RISK ACCEPTENCE**	-		**2**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
91	**441-4**	QDMS Software Maintanence Service	Failure of the process due to the failure to follow up updates and license periods	**1**	**1**	**1**	**2**	**2**	**1**	**2**	**2**	**5**	**LOW**	Updates are followed by IT, and license periods are followed by Purchasing Unit.	**RISK ACCEPTENCE**	-		**1**		**1**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
92	**441-5**	Ensemble Software Maintanence Service	Failure of the process due to the failure to follow up updates and license periods	**1**	**1**	**1**	**2**	**2**	**1**	**2**	**2**	**5**	**LOW**	Updates are followed by IT, and license periods are followed by Purchasing Unit.	**RISK ACCEPTENCE**	-		**1**		**1**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
93	**442-1**	GSM Communication Service	Customer may not reach by telephone due to a connection problem.	**1**	**2**	**1**	**2**	**3**	**2**	**4**	**6**	**12**	**LOW**	Communication is also available via fixed power plant.	**RISK ACCEPTENCE**	-		**1**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
94	**442-2**	Advertising Services	Advertising service provider may leak information of company's marketing strategy to competitors.	**3**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**15**	**LOW**	NDA (Non Disclosure Agreement) is signed with all suppliers.	**RISK ACCEPTENCE**	-		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
95	**442-3**	Career Web Site Service	Due to a power failure, candidates cannot access the career website	**1**	**2**	**1**	**2**	**3**	**2**	**4**	**6**	**12**	**LOW**	UPS system available for power failure.	**RISK ACCEPTENCE**	-		**1**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
96	**442-4**	Media Monitoring Service	Company's social media account may be hacked and hackers may share some posts against the company.	**3**	**1**	**3**	**2**	**2**	**3**	**2**	**2**	**21**	**LOW**	Media Monitoring service is outsourced and the company intervenes immediately when there is an attack. Experienced only once in 3 years	**RISK ACCEPTENCE**	-		**3**		**3**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
97	**443-1**	Strategic Management Consulting Service	Advertising service provider may leak information of company's marketing strategy to competitors.	**3**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**15**	**LOW**	NDA (Non Disclosure Agreement) is signed with all consultants.	**RISK ACCEPTENCE**	-		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

98	**443-2**	Quality Management Systems Consulting Service	Since QMS Consultant can access the firm's documentation platform remotely, he/she may leak the company know-how.	**3**	**3**	**3**	**1**	**1**	**9**	**3**	**3**	**45**	**MEDIUM**	Background checks are done and document transfers are tracked through the user's log records.	**MONITO-RING**	**M - 16**		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEP-TABLE RISK**	**CLO-SED**
99	**443-3**	Product Development Consulting Service	As a result of leakage of new product design information, the rival company may produce the new product before and introduced it to the market.	**3**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**30**	**MEDIUM**	NDA (Non Disclosure Agreement) is signed with all consultants.	**MONITO-RING**	**M - 17**		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEP-TABLE RISK**	**CLO-SED**
100	**444-1**	Fire Detection and Alarm System Maintenance Service	Due to failure to follow the maintenance of the fire extinguishing system there may be equipment failures may be in the event of a fire, fire outbreak may occur.	**1**	**2**	**1**	**3**	**3**	**2**	**6**	**6**	**14**	**LOW**	Maintenance controls are carried out by procurement and administrative affairs, but also by the service provider. The likelyhood of occurrence is low.	**RISK ACCEP-TENCE**	**-**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEP-TABLE RISK**	**CLO-SED**
101	**444-2**	Precision Air Conditioner Maintanence Service	Failure of the air conditioner in the server room due to lack of periodic maintenance. Failure of servers as a result.	**1**	**1**	**1**	**3**	**3**	**1**	**3**	**3**	**7**	**LOW**	Maintenance service is taken every 2 months and alarm system is activated when air conditioner is not working.	**RISK ACCEP-TENCE**	**-**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEP-TABLE RISK**	**CLO-SED**
102	**444-3**	UPS Maintanence Service	As a result of failure to perform a periodic maintenance contract may result in malfunction.	**1**	**3**	**1**	**1**	**3**	**3**	**3**	**9**	**15**	**LOW**	Periodic maintenance contract has been made and is followed up by technical unit responsible.	**RISK ACCEP-TENCE**	**-**		**1**		**1**	**1**	**3**	**0**	**0**	**0**	**0**	**ACCEP-TABLE RISK**	**CLO-SED**
103	**445-1**	Cleaning Service	Cleaning staff may enter to unauthorized areas and get an access to confidential information.	**1**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**10**	**LOW**	The areas where cleaning personnel can enter are defined, controlled by secure pass access system	**PROJECT**	**P-18**		**1**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**5**	**ACCEP-TABLE RISK**	**CLO-SED**
104	**445-2**	Security Service	Due to insufficient safety precautions and lack of burglar alarm, there may be a theft case.	**1**	**4**	**3**	**2**	**2**	**12**	**8**	**8**	**28**	**MEDIUM**	Security service is outsourced. This risk is transferred to security company.	**TRANSFER**	**-**		**1**		**3**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEP-TABLE RISK**	**CLO-SED**
105	**551-1**	Strategical Management	Disadvantage in competition due to disclosure of short-medium and long-term starategic plans.	**3**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**15**	**LOW**	Strategic plans are labeled as secret, and shared with only certain people from the management staff.	**RISK ACCEP-TENCE**	**-**		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEP-TABLE RISK**	**CLO-SED**

106	**551-2**	Systems Monitoring	Disruptions in the system due to lack of meeting notes related to decisions taken in Management Review meeting.	**1**	**2**	**1**	**3**	**3**	**2**	**6**	**6**	**14**	**LOW**	Decisions are transferred to the minutes with the approval of the participants during the meeting.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
107	**551-3**	Operational Overview	Disruption of integration due to lack of participation of a process owner in the Operational Overview meeting	**1**	**2**	**1**	**3**	**3**	**2**	**6**	**6**	**14**	**LOW**	If the process owner can not attend the meeting, another staff from the related departmen attends on behalf of him/her.	**PROJECT**	**P-19**		**1**	**1**	**1**	**3**	**3**	**1**	**3**	**3**	**7**	**ACCEPTABLE RISK**	**CLOSED**
108	**552-1**	Document Control	Documents may not be updated, due to periodic reviews are not made.	**1**	**5**	**1**	**3**	**3**	**5**	**15**	**15**	**35**	**MEDIUM**	Periodic updates with scheduled tasks in our document management system are made and approved by the document owner.	**MONITORING**	**M-18**		**1**		**1**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
109	**552-2**	Record Control	Data loss due to non-backup of records	**2**	**2**	**1**	**2**	**3**	**2**	**4**	**6**	**24**	**LOW**	Records are kept on the file server and backed up daily.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
110	**552-3**	Reporting Management	Sharing reports including secret information with wrong people.	**3**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**15**	**LOW**	The reporting matrix is available, as well as files belonging to reports containing highly confidential information are encrypted.	**RISK ACCEPTENCE**	**-**		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
111	**552-4**	Correspondences Tracking	Due to lack of a tracking system long response and completion times for regulatory commitments.	**2**	**1**	**1**	**2**	**3**	**1**	**2**	**3**	**12**	**LOW**	A correspondence and commitment tracking software is in use	**RISK ACCEPTENCE**	**-**		**2**		**1**	**2**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
112	**553-1**	Human Resources Management	Cvs belonging to the job candidates may be taken by unauthorized persons.	**1**	**3**	**3**	**1**	**1**	**9**	**3**	**3**	**15**	**LOW**	The files of job applications are kept under the responsibility of 2 certain personnel in HR department.	**RISK ACCEPTENCE**	**-**		**1**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
113	**553-2**	Information Technology Management	Unauthorized access to confidential information due to the fact that information privacy classification is not clear	**2**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**20**	**LOW**	Information security officer has been appointed as the primary responsible. All information is labeled according to their level of confidentiality.	**RISK ACCEPTENCE**			**2**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
114	**553-3**	Risk Management	The penetration of the virus into the computer and the spread of confidential information as a result of counterfait software / program installation of the staff	**3**	**1**	**3**	**1**	**1**	**3**	**1**	**1**	**15**	**LOW**	Staff is not allowed to install any program by the restricted network settings. It can be only installed by the IT department if needed.	**RISK ACCEPTENCE**	**-**		**3**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
115	**553-4**	Financial Management	Non-compliance with financial audit due to data entry error in financial indicators.	**2**	**2**	**1**	**3**	**2**	**2**	**6**	**4**	**24**	**LOW**	The reports are published after 3 different units review them.	**RISK ACCEPTENCE**	**-**		**2**		**1**	**3**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

116	**554-1**	Customer Relationship Management	Failure to respond to a complaint as a result of incorrect access to the help desk program where customer complaints are received, customer dissatisfaction	**1**	**2**	**1**	**1**	**3**	**2**	**2**	**6**	**10**	**LOW**	It is unlikely that customers will have their complaints coming directly from the web.	**RISK ACCEPTENCE**	**-**		**1**		**1**	**1**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
117	**554-2**	Supply Chain Management	In the absence of a production planning engineer, the production plan is carried out by unqualified personnel. Delay of shipments due to incomplete raw material demand.	**1**	**2**	**2**	**3**	**3**	**4**	**6**	**6**	**16**	**LOW**	Cross-competence for all processes has been acquired and there is a deputation matrix.	**RISK ACCEPTENCE**	**-**		**1**		**2**	**3**	**3**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
118	**554-3**	Project Management	Information security violations may occur in the project management process as the project objectives do not include information security objectives.	**2**	**2**	**3**	**1**	**1**	**6**	**2**	**2**	**20**	**LOW**	The project objectives have been prepared in accordance with the information security policy and the information security risks are also discussed in project risk analysis.	**RISK ACCEPTENCE**	**-**		**2**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
119	**554-4**	Production Management	Production of counterfeit products by illegal production as a result of theft	**3**	**2**	**2**	**1**	**1**	**4**	**2**	**2**	**24**	**LOW**	Access to the production site is only done by authorized personnel via turnstile. And the production site is constantly monitored by camera.	**RISK ACCEPTENCE**	**-**		**3**		**2**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
120	**555-1**	Auditing Management	Internal audit team members may not conduct regular audits to some departments due to personal relationships or do not report nonconformities.	**1**	**4**	**2**	**2**	**2**	**8**	**8**	**8**	**24**	**LOW**	Internal audit reports are compared with external audit reports and consistency analysis is performed.	**RISK ACCEPTENCE**	**-**		**1**		**2**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
121	**555-2**	Performance Management	Dissemination of salary and salary increase information due to lack of access controls in the performance evaluation process.	**1**	**3**	**3**	**1**	**1**	**9**	**3**	**3**	**15**	**LOW**	Performance evaluation is done through the system and the entries to the system can be done by passwords.	**RISK ACCEPTENCE**	**-**		**1**		**3**	**1**	**1**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**
122	**555-3**	Nonconformity and Improvement Management	Internal audit team members may not conduct regular audits to some departments due to personal relationships or do not report nonconformities.	**1**	**4**	**2**	**2**	**2**	**8**	**8**	**8**	**24**	**LOW**	Internal audit reports are compared with external audit reports and consistency analysis is performed.	**RISK ACCEPTENCE**	**-**		**1**		**2**	**2**	**2**	**0**	**0**	**0**	**0**	**ACCEPTABLE RISK**	**CLOSED**

APPENDIX B: CONTROL EFFICIENCY MONITORING PLAN

Table B.1. Control efficiency monitoring plan.

NO	RISK	IMPACTED ASSETS			MONITORING				
		NO	ASSET NAME	ASSET DEFINITION	WHAT	HOW	FREQUENCY	WHO	RECORD
M-1	Improper reports and incorrect strategic decisions due to user's incorrect data entry	111-2	SAP HANA Database	An in-memory, column-oriented, relational database	Data consistency	Automated cross-checks	Consistently	System	System reports
M-2	Data distortion due to integration with other business solutions and softwares.	111-3	SAP GUI Database	The database used for remote access to the SAP central server in a company network.	Data accuracy	Full cycle integration tests	Consistently	System	System reports
M-3	Attackers could gain unrestricted access to an entire database via SQL injection.	111-5	Head Office Server Database	The database where all supply chain data is available	Unauthorized queries injected via web applications.	Query-level access control detection	Consistently	Third-party detection system	System reports
M-4	System crash due to denied access to database because of frequent power cuts.	111-6	Back-Up Database	The database that enables the creation of a duplicate instance or copy of a database in case the primary database crashes, is corrupted or is lost.	UPS and generator running-up time	Tests/controls during periodic maintenance	Every 3 months	Technical Service Personnel	Periodic maintenance report

M-5	Incorrect drug formula due to non-compliance with detected measurement frequency	112-20	Drug Formulation	Specific ratios of active substance and other chemical components in the content of a drug	Periodic calibration of inline measurment equipment	Certified comparison tests	Monthly	Production Quality Engineer	Periodic calibration report
M-6	Data loss due to problems in disks.	112-27	All Data Files on File Server	All files located on fileserver	Data storage	Automated continuous control on the disk	Daily	IT Network Engineer	System reports
M-7	Failure to register as a result of not starting the camera program at the end of working hours due to the office assistant's absence.	112-29	Camera Records	Security camera recordings of entrances and exits	Running record	Automated continuous control and alarm system	Consistently	Security Officer	Alarm system reports
M-8	Security openings due to failure of the operating system updates and consequently hacker attacks	221-1	Notebooks	Computers debited to employees	Firewall	Penetration tests	Every 3 months	IT Network Engineer	Penetration test reports
M-9	The loss of data within our servers as a result of flooding and our system will not work for a certain period of time	221-3	Head Office Servers	Head Office Servers	Contact with liquid	Liquid sensor and alarm systems	Consistently	Administrative Affairs Responsible	Alarm system reports
M-10	Servers overheating due to failure of the air conditioner and temperature values can not be controlled	221-4	Web App Server	Web App Server	Server room ambient temperature	Heat sensor and alarm systems	Consistently	Administrative Affairs Responsible	Alarm system reports

M-11	Unauthorized personnel entry into the server room or an attempt to be entered forcibly due to a data privacy violation and data theft.	221-5	Backup Database Server	Backup Database Server	Access control system	Matching logs with access rights	Monthly	Administrative Affairs Responsible	Match-Up control reports
M-12	Failure to retrieve backups due to inadequate backup system	223-1	Backup Cartridges	Tapes in which back up data is stored	Backup Data	Command Check	Consistently	System	Backup log
M-13	Due to software malfunction, the logs can not be erased. Backups may not be taken because of the full memory.	223-3	Portable Hard Drives	External hard drives that are used by employees	Disk occupancy rate	Log cleanup command	Daily	IT Network Engineer	Control forms
M-14	Attackers may get their identity information authorized with the help of spoofing through emails or Ips	224-4	VPN Appliance	Network device which provides load balancing with strong security features.	VPN Access rights	Access authorization workflow	In case of VPN access need	IT Network Engineer	VPN access logs
M-15	An unauthorized person may find a lost security pass and enter the facility.	225-8	Entrance Turnstile	Entrance Turnstile	Access control system	Random checks and camera records	3 times a day	Security Officer	Control reports
M-16	Since QMS Consultant can access the firm's documentation platform remotely, he/she may leak the company know-how.	443-2	Quality Management Systems Consulting Service	Quality Systems audits and Maintenance of Quality Systems	Access control system and document transfers	Monitoring	Consistently	IT Network Engineer	Quality Systems login reports and document transfer reports

M-17	As a result of leakage of new product design information, the rival company may produce the new product before and introduced it to the market.	443-3	Product Development Consulting Service	New product design and laboratory service	Confidential information	Encrypted document/information sharings	Consistently	IT Manager	Information distribution tracking reports
M-18	Documents may not be updated, due to periodic reviews are not made.	552-1	Document Control	Identification, preparation, publication, distribution and revisions of documents	Documents Updates	Scheduled task assignment over system	Every 6 months	Quality Systems Engineer	Document Update and Revision Summary Reports

APPENDIX C: INFORMATION ASSETS INVENTORY

Table C.1. Information assets inventory.

Cat. ID	Sub Cat. ID	Varlık Alt Kat.	Asset ID	Asset Name	Asset Location	Asset Definition	Asset Owner	Asset Custodian	Asset Class	Replacement Value
1	11	Database	111-1	CRM Database	CRM Server	The database where the customer data and orders are available	IT Manager	CRM Specialist	Secret	3
			111-2	SAP HANA Database	SAP Applications Server	An in-memory, column-oriented, relational database	IT Manager	IT Specialist	Confidential	3
			111-3	SAP GUI Database	Head Office Server	The database used for remote access to the SAP central server in a company network.	IT Manager	IT Specialist	Confidential	3
			111-4	Web Database	Microsoft SQL Server	The database application designed to be managed and accessed through the Internet	IT Manager	IT Supervisor	Secret	3
			111-5	Head Office Server Database	Head Office Server	The database where all supply chain data is available	IT Manager	IT Supervisor	Secret	3
			111-6	Back-Up Database	HP Storage Units	The database that enables the creation of a duplicate instance or copy of a database in case the primary database crashes, is corrupted or is lost.	IT Manager	IT Specialist	Confidential	3

	12	Data File	112-1	Quality Management Systems Documents	QDMS Database	Procedures, instructions, process maps in the scope of Quality Management System	Quality Manager	Quality Supervisor	Internal Use Only	2
			112-2	Information Security Management Documents	QDMS Database	Procedures, instructions, process maps in the scope of Information Security Management System	Quality Manager	Quality Supervisor	Confidential	2
			112-3	Information Security Risk Management Records	QDMS Database	Risk Analysis studies in the scope of Information Security Management System	Quality Manager	Quality Supervisor	Confidential	2
			112-4	Nonconformity Records	QDMS Database	Customer complaints, corrective and preventive actions, product return records	Quality Manager	Quality Supervisor	Confidential	2
			112-5	Calibration Records	QDMS Database	Calibration and verification records of measuring devices	Quality Manager	Quality Supervisor	Confidential	2
			112-6	Project Records	QDMS Database	R&D and Improvement Projects Records	Project Manager	Project Specialist	Confidential	2
			112-7	Quality Control Records	QDMS Database	Quality Plan, process and product quality control records	Quality Manager	Quality Supervisor	Confidential	2
			112-8	Corporate Performance Management Records	QDMS Database	Coorparate scorecard, department scorecards and process activities monitoring table, customer satisfaction surveys	Quality Manager	Quality Supervisor	Confidential	2
			112-9	Payroll Information	SAP HR Module	Personnel salary and benefits information	HR Manager	Payroll and Benefits Specialist	Confidential	2
			112-10	Business Contracts	QDMS Database	Contracts with supplier, subcontractor manufacturer, health ministry and FDA	Finance Manager	Accounting Specialist	Secret	2
			112-11	Personnel Affairs Documents	QDMS Database	Personnel files of all employees	HR Manager	Recruitment Specialist	Confidential	2
			112-12	IT Equipment Records	QDMS Database	All failure reports, licences, contracts etc related to IT equipment	IT Manager	IT Supervisor	Internal Use Only	1
			112-13	Proxy Permission List	QDMS Database	Given access rights for related websites	IT Manager	IT Supervisor	Confidential	1
			112-14	Health Ministry Correspondence Files	QDMS Database	Correspondences related to official permissons, legislations, regulations etc	Inhouse Lawyer	Contract Manager	Secret	1

			112-15	Customer Information	CRM Database	Tax ID number, adressess, phone number etc communication information	Marketing Manager	Customer Relationship Specialist	Secret	3
			112-16	Approved Vendor List	SAP MM Module	List of our suppliers who have been certified to meet our quality standards	Purchasing Manager	Purchasing Specialist	Internal Use Only	2
			112-17	Vendor Information	SAP MM Module	Tax ID number, adressess, phone number etc communication information	Purchasing Manager	Purchasing Specialist	Internal Use Only	2
			112-18	Financial Statements	BI Database	Declaration, income statement, balance sheet, cash flow statement etc.	Finance Manager	Budget Planning Specialist	Confidential	2
			112-19	Formal Reports	Fileserver	Reports which are submitted to Health Ministry including sales information	Finance Manager	Accounting Specialist	Confidential	2
			112-20	Drug Formulation	SAP Production Module	Specific ratios of active substance and other chemical components in the content of a drug	R&D Manager	R&D Specialist	Secret	3
			112-21	Production Reports	SAP Production Module	Monthly, weekly production plans, including shipment	Production Manager	Industrial Engineer	Internal Use Only	1
			112-22	Machine Information and Instructions for Use	Fileserver	Instruction, specification, calibration information of machines	Production Manager	Industrial Engineer	Internal Use Only	1
			112-23	Change Request Records	Sharepoint	Changes for improvement of a product or a process	Project Manager	Project Specialist	Confidential	1
			112-24	Inventory Information	QDMS	Inventory, raw material, final product,wastage etc	Warehouse Supervisor	Warehouse Specialist	Internal Use Only	1
			112-25	Shipment Reports	SAP MM Module	Weekly, monthly, yearly drug shipment reports	Logistics Manager	Logistics Specialist	Confidential	1
			112-26	Operational Dashboard	BI Database	KPI report of all functions	Quality Manager	Quality Supervisor	Confidential	1
			112-27	All Data Files on File Server	Fileserver	All files located on fileserver	IT Manager	IT Supervisor	Confidential	3
			112-28	All Data Files on Sharepoint	Sharepoint	All files located on sharepoint	IT Manager	IT Supervisor	Confidential	3

			112-29	Camera Records	Sharepoint	Security camera recordings of entrances and exits	Administrative Affairs Manager	Security Officer	Confidential	2
	13	Printed Material	113-1	ISO 9001 Quality Documents	Quality Systems Department/Cabinet	Certificates	Quality Manager	Quality Supervisor	Internal Use Only	1
			113-2	Invoices	Finance Department/Cabinet	Invoices from suppliers and given to customers	Finance Manager	Accounting Specialist	Confidential	1

APPENDIX D: PHYSICAL ASSETS INVENTORY

Table D.1. Physical assets

Cat. ID	Sub Cat. ID	Varlık Alt Kat.	Asset ID	Asset Name	Asset Location	Asset Definition	Asset Owner	Asset Custodian	Replacement Value
2	21	Computer Equipments	221-1	Notebooks	Inside and outside of the company	Computers debited to employees	IT Manager	IT Specialist	2
			221-2	Printers	Inside of the company including head 92ffice and regional offices	Printers	IT Manager	IT Specialist	2
			221-3	Head Office Servers	Head Office	Head Office Servers	IT Manager	IT Specialist	3
			221-4	Web App Server	Head Office	Web App Server	IT Manager	IT Specialist	3
			221-5	Backup Database Server	Head Office	Backup Database Server	IT Manager	IT Specialist	3
			221-6	BPC Database Server	Head Office	BPC Database Server	IT Manager	IT Specialist	3
			221-7	CRM Database Server	Head Office	CRM Database Server	IT Manager	IT Specialist	3
			221-8	SAP Applications Server	Head Office	SAP Applications Server	IT Manager	IT Specialist	3
	22	Communication Equipments	222-1	Mobile Phones	Inside and outside of the company	Mobile phones debited to employees	IT Manager	IT Specialist	2
			222-3	IP Telephones	Inside of the company including head 92ffice and regional offices	IP Telephones	IT Manager	IT Specialist	1
	23	Recording Media	223-1	Backup Cartridges	Server Rooms	Tapes in which back up data is stored	IT Manager	IT Specialist	3
			223-2	CCTV Server	Head Office	Servers in which camera records are stored	IT Manager	IT Specialist	2
			223-3	Portable Hard Drives	Inside and outside of the company	External hard drives that are used by employees	IT Manager	IT Specialist	2

			223-4	SSD	Notebooks	Storage unit	IT Manager	IT Specialist	3
	24	Network Equipments	224-1	Firewall Machine	Head Office and Regional Offices	A 93ffi that protects a network or a system from unauthorized 93ffice.	IT Manager	IT Specialist	3
			224-2	Accesspoints	Head Office and Regional Offices	Devices that allows wireless devices to connect to a network	IT Manager	IT Specialist	1
			224-3	Routers	Head Office and Regional Offices	Devices thatdirect data traffic between 2 or more networks	IT Manager	IT Specialist	2
			224-4	VPN Appliance	Head Office and Regional Offices	Network device which provides load balancing with strong security features.	IT Manager	IT Specialist	2
			224-5	Switches	Head Office and Regional Offices	Devices that channel incoming data from any of multiple input ports to the specific output port that will take it toward its intended destination.	IT Manager	IT Specialist	1
			224-6	Gateways	Head Office and Regional Offices	Data communication devices that provide a remote network with connectivity to a host network	IT Manager	IT Specialist	2
	25	Other	225-1	Barcode Readers	Warehouses in head 93ffice and regional offices	Barcode Readers	Warehouse Supervisor	Warehouse Specialist	2
			225-2	Cameras	Outside and inside of Head Offices and regional offices	Cameras	Administrative Affairs Manager	Security Officer	2
			225-3	Raw Materials	Warehouses in production site	Raw materials used in pharmaceutical production	Warehouse Supervisor	Warehouse Specialist	2
			225-4	Spare Parts	Warehouses in head 93ffice and regional offices	Spare parts used in machine failures and maintenance	Warehouse Supervisor	Warehouse Specialist	2

			225-5	Fire Detection and Alarm System Equipments	Head Office and Regional Offices	Fire Detection and Alarm System Equipments	Administrative Affairs Manager	Security Officer	1
			225-6	Finished Products	Warehouses in production site	Packaged drug	Warehouse Supervisor	Warehouse Specialist	3
			225-7	UPS	Head Office and Regional Offices	Uninterruptible power supply	Administrative Affairs Manager	Electrician	1
			225-8	Entrance Turnstile	Main entrance of head 94ffice and regional offices	Entrance Turnstile	Administrative Affairs Manager	Security Officer	2
			225-9	Laboratory Equipments	Laboratuary in production site	Laboratory Equipments	R&D Manager	R&D Specialist	1
			225-10	Production Machines	Production site	Production Machines	Production Manager	Industrial Engineer	3
			225-11	Coding Machines	Production site	Machines that personalize the each drug package by unique codes	Production Manager	Industrial Engineer	3

APPENDIX E: SOFTWARE ASSETS INVENTORY

Table E.1. Software assets inventory.

Cat. ID	Sub Cat. ID	Varlık Alt Kat.	Asset ID	Asset Name	Asset Location	Asset Definition	Asset Owner	Asset Custodian	Replacement Value
3	31	Operating System	331-1	Windows	Microsoft Online System	Windows 2010 and 2013 Operating System	IT Manager	IT Specialist	2
			331-2	Android	Technical Personnel’s Tablets	Android Operating System	IT Manager	IT Specialist	2
	32	Application Software	332-1	Fiori Mobile	Users’ devices	A set of applications that are used in regular business functions like work approvals, financial apps, calculation apps and various self-service apps	IT Manager	IT Specialist	2
			332-2	Cryptolog	Fileserver	Log management system	IT Manager	IT Specialist	1
			332-3	MS Office Programs	Microsoft Online System	Word, excel, powerpoint etc	IT Manager	IT Specialist	1
			332-4	Web Server Software	Data Management System	Proxy, webapp etc	IT Manager	IT Specialist	3
			332-5	SAP	SAP Server in Head Office	All ERP Modules	IT Manager	IT Specialist	3
			332-6	QDMS	QDMS Server in Head Office	Document approval work flow, document distribution etc	IT Manager	IT Specialist	1
			332-7	Exchange Server	Microsoft Online System	Mail and calendering server	IT Manager	IT Specialist	1

			332-8	TrendMicro	Head Office Server	Antivirus Software	IT Manager	IT Specialist	3
			332-9	Microsoft Office 365	Microsoft Online System	Online version of the traditional installed version of Microsoft Office software.	IT Manager	IT Specialist	1
	33	System Software	333-1	SAP System Software	SAP Server in Head Office	ERP System software	IT Manager	IT Specialist	2
			333-2	Master PC Systems Software	Master PC	Master PC Systems Software	IT Manager	IT Specialist	2
			333-3	Back Up Software	Fileserver	Avamar	IT Manager	IT Specialist	1
			333-4	Compilers	Fileserver	Software that transforms computer code written in one programming language (the source language) into another programming language (the target language).	IT Manager	IT Specialist	3
			333-5	Debuggers	Fileserver	Software that is used to find bugs in other programs	IT Manager	IT Specialist	3
			333-6	Browsers	Fileserver	Software that is used to view web pages on the internet	IT Manager	IT Specialist	3
			333-7	Disk Cleaner	Fileserver	A 96icrosoft software that removes the unnecessary files and increase disk space on a computer's hard drive.	IT Manager	IT Specialist	1
			333-8	Remote Access Software	SAP Server in Head Office	TeamViewer, Any Desk etc	IT Manager	IT Specialist	1

APPENDIX F: SERVICE ASSETS INVENTORY

Table F.1. Service assets inventory.

Cat. ID	Sub Cat. ID	Varlık Alt Kat.	Asset ID	Asset Name	Service Supporter	Asset Definition	Asset Owner	Asset Custodian	Replacement Value
4	41	Information Services	441-1	Customer Support Service	XY Technology Solutions	Support and Maintanence	IT Manager	IT Supervisor	1
			441-2	SAP Software Maintanence Service	SAP Partner	SAP Module Support and BASIS Service	IT Manager	IT Supervisor	2
			441-3	SAP Licence Maintanence Service	SAP Partner	SAP Licence Maintanence	IT Manager	IT Supervisor	2
			441-4	QDMS Software Maintanence Service	BIMSER	Support and Maintanence of Software	Quality Manager	Quality Supervisor	1
			441-5	Ensemble Software Maintanence Service	BIMSER	Support and Maintanence of Software	Quality Manager	Quality Supervisor	1
	42	Communication Services	442-1	GSM Communication Service	Turk Telekom	Mobile Communication Service	Administrative Affairs Manager	Department Managers	1
			442-2	Advertising Services	ABC Advertisement	Advertising layout and typography of the company	Marketing Manager	Marketing Supervisor	3

			442-3	Career Web Site Service	Diverse Effect	Direct job applications	HR Manager	Recruitment Specialist	1
			442-4	Media Monitoring Service	MMC	Monitoring media broadcasts	Marketing Manager	Marketing Supervisor	3
	43	Consulting Services	443-1	Strategic Management Consulting Service	ABBD Turkey	Strategic management support	General Manager	Vice President	1
			443-2	Quality Management Systems Consulting Service	RL QA Quality Systems	Quality Systems audits and Maintanence of Quality Systems	Quality Manager	Quality Supervisor	1
			443-3	Product Development Consulting Service	NP Consultancy	New product design and laboratory service	R&D Manager	R&D Specialist	3
	44	Technical Services	444-1	Fire Detection and Alarm System Maintanence Service	FD Mechanical Heat and Alarm Systems	Periodic maintenance of fire extinguishing equipment	Administrative Affairs Manager	HSE Specialist	1
			444-2	Precision Air Conditioner Maintanence Service	FD Mechanical Heat and Alarm Systems	Periodic maintenance of air conditions	Administrative Affairs Manager	HSE Specialist	1
			444-3	UPS Maintanence Service	Power Electronics	Uninterruptible power supply	Administrative Affairs Manager	Electrician	1
	45	Other	445-1	Cleaning Service	MERS Cleaning	Office cleaning services	Administrative Affairs Manager	Administrative Affairs Specialist	1
			445-2	Security Service	Guardian Security	Facility security services	Administrative Affairs Manager	Security Officer	1

APPENDIX G: PROCESS ASSETS INVENTORY

Table G.1. Process assets inventory.

Cat. ID	Sub Cat. ID	Varlık Alt Kat.	Asset ID	Asset Name	Asset Definition	Asset Owner	Asset Custodian	Replacement Value
5	51	STRATEGICAL PLANNING	551-1	Strategical Management	Long term, medium term, short term plans of company, objectives	General Manager	Vice President	3
			551-2	Systems Monitoring	Management review meeting	General Manager	General Manager Assistant	1
			551-3	Operational Overview	Regular meetings like production , quality, department meetings	General Manager	General Manager Assistant	1
	52	INFORMATION MANAGEMENT	552-1	Document Control	Identification, preparation, publication, distribution and revisions of documents	Quality Manager	Quality Supervisor	1
			552-2	Record Control	Classification, identification and preservation of records	Quality Manager	Quality Supervisor	1
			552-3	Reporting Management	Reporting Matrix	Quality Manager	Quality Supervisor	3
			552-4	Correspondences Tracking	Incoming outgoing document management procedure, paperwork request and transfer slips	General Manager	General Manager Assistant	2

	53	RESOURCE MANAGEMENT	553-1	Human Resources Management	Employment management procedure, application and evaluation forms, annual leave forms etc.	Human Resources Manager	Human Resources Supervisor	1
			553-2	Information Technology Management	Hardware Software Management Procedures, forms and lists of IT jobs, topology etc.	IT Manager	IT Supervisor	1
			553-3	Risk Management	Risk Management Documents, processes, ISMS manual etc.	Quality Manager	Quality Supervisor	3
			553-4	Financial Management	Budgeting system and budget revision process	Finance Manager	Accounting Specialist	2
	54	SERVICE MANAGEMENT	554-1	Customer Relationship Management	Customer Data Identification, Order Management, Customer Support Management etc.	Marketing Manager	Customer Relationship Specialist	1
			554-2	Supply Chain Management	Demand Planning, Supply Planning and Purchasing, Supplier Evaluation etc.	Purchasing Manager	Purchasing Specialist	1
			554-3	Project Management	Project application, plan, execution, completion etc.	Project Manager	Department Managers	2
			554-4	Production Management	Production planning, realization of production, making products ready for packing and shipping	Production Manager	Industrial Engineer	3
	55	IMPROVEMENT MANAGEMENT	555-1	Auditing Management	Internal and external audit procedures, audit plans, audit reports etc.	Quality Manager	Quality Supervisor	1

			555-2	Performance Management	Process performance monitoring procedure, department scorecards, target tracking, performance management process, performance evaluation procedure etc	HR Manager	HR Supervisor	1
			555-3	Nonconformity and Improvement Management	Customer complaints management procedure, Corrective and Proactive Actions (CAPA) management procedure, business process change management procedure	Quality Manager	Quality Supervisor	1

APPENDIX H: VULNERABILITIES

Table H.1. Vulnerabilities.

TYPE	EXAMPLES OF VULNERABILITIES	EXAMPLES OF THREATS	ABBREVIATIONS
Hardware	Insufficient maintenance/faulty installation of hardware	Breach of information system maintainability	Insufficient maintenance/faulty installation of storage media
	Lack of periodic replacement schemes	Destruction of equipment or media	Lack of periodic replacement schemes
	Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing	Susceptibility to humidity, dust, soiling
	Sensitivity to electromagnetic radiation	Electromagnetic radiation	Sensitivity to electromagnetic radiation
	Lack of efficient configuration change control	Error in use	Lack of efficient configuration change control
	Susceptibility to voltage variations	Loss of power supply	Susceptibility to voltage variations
	Susceptibility to temperature variations	Meteorological phenomenon	Susceptibility to temperature variations
	Unprotected storage	Theft of media or documents	Unprotected storage
	Lack of care at disposal	Theft of media or documents	Lack of care at disposal
	Uncontrolled copying	Theft of media or documents	Uncontrolled copying
Software	No or insufficient software testing	Abuse of rights	No or insufficient software testing
	Well-known flaws in the software	Abuse of rights	Well-known flaws in the software
	No 'logout' when leaving the workstation	Abuse of rights	No 'logout' when leaving the workstation
	Disposal or reuse of storage media without proper erasure	Abuse of rights	Disposal or reuse of storage media without proper erasure
	Lack of audit trail	Abuse of rights	Lack of audit trail
	Wrong allocation of access rights	Abuse of rights	Wrong allocation of access rights
	Widely-distributed software	Corruption of data	Widely-distributed software

	Applying application programs to the wrong data in terms of time	Corruption of data	Applying application programs to the wrong data in terms of time
	Complicated user interface	Error in use	Complicated user interface
	Lack of documentation	Error in use	Lack of documentation
	Incorrect parameter set up	Error in use	Incorrect parameter set up
	Incorrect dates	Error in use	Incorrect dates
	Lack of identification and authentication mechanisms like user authentication	Forging of rights	Lack of identification and authentication mechanisms like user authentication
	Unprotected password tables	Forging of rights	Unprotected password tables
	Poor password management	Forging of rights	Poor password management
	Unnecessary services enabled	Illegal processing of data	Unnecessary services enabled
	Immature or new software	Software malfunction	Immature or new software
	Unclear or incomplete specifications for developers	Software malfunction	Unclear or incomplete specifications for developers
	Lack of effective change control	Software malfunction	Lack of effective change control
	Uncontrolled downloading and use of software	Tampering with software	Uncontrolled downloading and use of software
	Lack of back-up copies	Tampering with software	Lack of back-up copies
	Lack of physical protection of the building, doors and windows	Theft of media or documents	Lack of physical protection of the building, doors and windows
	Failure to produce management reports	Unauthorised use of equipment	Failure to produce management reports
Network	Lack of proof of sending or receiving a message	Denial of actions	Lack of proof of sending or receiving a message
	Unprotected communication lines	Eavesdropping	Unprotected communication lines
	Unprotected sensitive traffic	Eavesdropping	Unprotected sensitive traffic
	Poor joint cabling	Failure of telecommunication equipment	Poor joint cabling
	Single point of failure	Failure of telecommunication equipment	Single point of failure
	Lack of identification and authentication of sender and receiver	Forging of rights	Lack of identification and authentication of sender and receiver

	Insecure network architecture	Remote spying	Insecure network architecture
	Transfer of passwords in clear	Remote spying	Transfer of passwords in clear
	Inadequate network management (resilience of routing)	Saturation of the information system	Inadequate network management (resilience of routing)
	Unprotected public network connections	Unauthorised use of equipment	Unprotected public network connections
Personnel	Absence of personnel	Breach of personnel availability	Absence of personnel
	Inadequate recruitment procedures	Destruction of equipment or media	Inadequate recruitment procedures
	Insufficient security training	Error in use	Insufficient security training
	Incorrect use of software and hardware	Error in use	Incorrect use of software and hardware
	Lack of security awareness	Error in use	Lack of security awareness
	Lack of monitoring mechanisms	Illegal processing of data	Lack of monitoring mechanisms
	Unsupervised work by outside or cleaning staff	Theft of media or documents	Unsupervised work by outside or cleaning staff
	Lack of policies for the correct use of telecommunications media and messaging	Unauthorised use of equipment	Lack of policies for the correct use of telecommunications media and messaging
Site	Inadequate or careless use of physical access control to buildings and rooms	Destruction of equipment or media	Inadequate or careless use of physical access control to buildings and rooms
	Location in an area susceptible to flood	Flood	Location in an area susceptible to flood
	Unstable power grid	Loss of power supply	Unstable power grid
	Lack of physical protection of the building, doors and windows	Theft of equipment	Lack of physical protection of the building, doors and windows
Organization	Lack of formal procedure for user registration and de-registration	Abuse of rights	Lack of formal procedure for user registration and de-registration
	Lack of formal process for access right review (supervision)	Abuse of rights	Lack of formal process for access right review (supervision)
	Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties	Abuse of rights	Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties

	Lack of procedure of monitoring of information processing facilities	Abuse of rights	Lack of procedure of monitoring of information processing facilities
	Lack of regular audits (supervision)	Abuse of rights	Lack of regular audits (supervision)
	Lack of procedures of risk identification and assessment	Abuse of rights	Lack of procedures of risk identification and assessment
	Lack of fault reports recorded in administrator and operator logs	Abuse of rights	Lack of fault reports recorded in administrator and operator logs
	Inadequate service maintenance response	Breach of information system maintainability	Inadequate service maintenance response
	Lack or insufficient Service Level Agreement	Breach of information system maintainability	Lack or insufficient Service Level Agreement
	Lack of change control procedure	Breach of information system maintainability	Lack of change control procedure
	Lack of formal procedure for ISMS documentation control	Corruption of data	Lack of formal procedure for ISMS documentation control
	Lack of formal procedure for ISMS record supervision	Corruption of data	Lack of formal procedure for ISMS record supervision
	Lack of formal process for authorization of public available information	Data from untrustworthy sources	Lack of formal process for authorization of public available information
	Lack of proper allocation of information security responsibilities	Denial of actions	Lack of proper allocation of information security responsibilities
	Lack of continuity plans	Equipment failure	Lack of continuity plans
	Lack of e-mail usage policy	Error in use	Lack of e-mail usage policy
	Lack of procedures for introducing software into operational systems	Error in use	Lack of procedures for introducing software into operational systems
	Lack of records in administrator and operator logs	Error in use	Lack of records in administrator and operator logs
	Lack of procedures for classified information handling	Error in use	Lack of procedures for classified information handling

	Lack of information security responsibilities in job descriptions	Error in use	Lack of information security responsibilities in job descriptions
	Lack or insufficient provisions (concerning information security) in contracts with employees	Illegal processing of data	Lack or insufficient provisions (concerning information security) in contracts with employees
	Lack of defined disciplinary process in case of information security incident	Theft of equipment	Lack of defined disciplinary process in case of information security incident
	Lack of formal policy on mobile computer usage	Theft of equipment	Lack of formal policy on mobile computer usage
	Lack of control of off-premise assets	Theft of equipment	Lack of control of off-premise assets
	Lack or insufficient 'clear desk and clear screen' policy	Theft of media or documents	Lack or insufficient 'clear desk and clear screen' policy
	Lack of information processing facilities authorization	Theft of media or documents	Lack of information processing facilities authorization
	Lack of established monitoring mechanisms for security breaches	Theft of media or documents	Lack of established monitoring mechanisms for security breaches
	Lack of regular management reviews	Unauthorised use of equipment	Lack of regular management reviews
	Lack of procedures for reporting security weaknesses	Unauthorised use of equipment	Lack of procedures for reporting security weaknesses
	Lack of procedures of provisions compliance with intellectual rights	Use of counterfeit or copied software	Lack of procedures of provisions compliance with intellectual rights

APPENDIX I: THREATS

Table I.1. Threats.

TYPES	THREAT	ORIGIN	ABBREVIATION
Physical damage	Fire	A,D,E	Fire
	Water damage	A,D,E	Water damage
	Pollution	A,D,E	Pollution
	Major accident	A,D,E	Major accident
	Destruction of equipment or media	A,D,E	Destruction of equipment or media
	Dust, corrosion, freezing	A,D,E	Dust, corrosion, freezing
Natural events	Climatic phenomenon	E	Climatic phenomenon
	Seismic phenomenon	E	Seismic phenomenon
	Volcanic phenomenon	E	Volcanic phenomenon
	Meteorological phenomenon	E	Meteorological phenomenon
	Flood	E	Flood
Loss of essential services	Failure of air-conditioning or water supply system	A,D	Failure of air-conditioning or water supply system
	Loss of power supply	A,D,E	Loss of power supply
	Failure of telecommunication equipment	A,D	Failure of telecommunication equipment

Disturbance due to Thermal radiation	Electromagnetic radiation	A,D,E	Electromagnetic radiation
	Thermal radiation	A,D,E	Thermal radiation
	Electromagnetic pulses	A,D,E	Electromagnetic pulses
Compromise of information	Interception of compromising interference signals	D	Interception of compromising interference signals
	Remote spying	D	Remote spying
	Eavesdropping	D	Eavesdropping
	Theft of media or documents	D	Theft of media or documents
	Theft of equipment	D	Theft of equipment
	Retrieval of recycled or discarded media	D	Retrieval of recycled or discarded media
	Disclosure	A,D	Disclosure
	Data from untrustworthy sources	A,D	Data from untrustworthy sources
	Tampering with hardware	D	Tampering with hardware
	Tampering with software	A,D	Tampering with software
	Position detection	D	Position detection
Technical failures	Equipment failure	A	Equipment failure
	Equipment malfunction	A	Equipment malfunction
	Saturation of the information system	A,D	Saturation of the information system
	Software malfunction	A	Software malfunction

	Breach of information system maintainability	A,D	Breach of information system maintainability
Unauthorised actions	Unauthorised use of equipment	D	Unauthorised use of equipment
	Fraudulent copying of software	D	Fraudulent copying of software
	Use of counterfeit or copied software	A,D	Use of counterfeit or copied software
	Corruption of data	D	Corruption of data
	Illegal processing of data	D	Illegal processing of data
Compromise of functions	Error in use	A	Error in use
	Abuse of rights	A,D	Abuse of rights
	Forging of rights	D	Forging of rights
	Denial of actions	D	Denial of actions
	Breach of personnel availability	A,D,E	Breach of personnel availability

APPENDIX J: ISMS ACTIVITY ACTION LIST

Table J.1. ISMS activity action list.

NO	ACTIVITY/PROJECT	Administrative Affairs Ma-	Contract Manager	Finance Manager	General Manager	HR Manager	Inhouse Lawyer	IT Manager	Logistics Manager	Marketing Manager	Process Improvement Ma-	Production Manager	Project Manager	Purchasing Manager	R&D Manager	Quality Manager	PLANNED END DATE	ACTUAL ENDING DATE	STATUS
P-1	Rules for the distribution of sensitive data on CRM database will defined and any attempts to overcome these rules will be blocked and reported.				P			R		P							28-Feb-15	23-Feb-15	Comple-ted
P-2	Due to accidental deletion, loss of data during an Office 365 migration and get a cloud-based data backup solution like Backupify.							R						P			6-Jun-15	30-May-15	Comple-ted
P-3	A job will be set up to check whether the parameter values contained in the integration are equivalent between the respective systems.			P		P		R	P	P			P	P		P	20-Mar-15	30-Mar-15	Comple-ted

P-4	Inline quality control automation will be provided in the processes. The related measurements will be made and reported by the system at specified frequencies and the defective products will be extracted out of the line.								P		P	P				R	12-Dec-15	27-Dec-15	Completed
P-5	A log program will be coded to keep track of the changes made to the documents.							R			p					P	16-Jan-16	29-Aug-15	Completed
P-6	Contract administation department is will be established				R	p	P							p			6-Apr-15	15-Apr-15	Completed
P-7	Counting will be done with RFID system and SAP integration and counting results can be reported from the system			P				P	R		P			P			3-Nov-18	2-Nov-15	Completed
P-8	Customer information is only kept in CRM database, all confidential information will be encrypted, and just authorized contacts will have access to relevant information.		P		P			P		R	P					P	7-May-15	30-Apr-15	Completed
P-9	System integration will be provided with Ministry of Health. Ministry of Health approval will be checked automatically. If there is not approval, SAP system will prevent shipment.		P					R	P								3-Jul-15	5-Jul-15	Completed

P-10	Goods receiving and goods issue processes will be carried out with barcode reader. Amounts of goods which are transferred or received will be reflected in the system simultaneously via wireless connection.	P							R					P			1-Aug-15	27-Jul-15	Completed
P-11	Encrypted printing will be provided, in order to ensure security of printed sensitive or confidential information. After a personnel send the job, it is held at the printer until he enters his passcode at the printer control panel.							R									22-Mar-15	15-Mar-15	Completed
P-12	Stand-By Servers Project				P			R	P		P		P				8-Nov-15	5-Nov-15	Completed
P-13	Random controls will be made with turnstile alarm system.	R										P				P	15-Feb-15	11-Feb-15	Completed
P-14	Fingerprint based access control system project	R						P							P	P	18-Sep-15	16-Sep-15	Completed
P-15	Only macros from trusted locations are enabled.If organisations have a business requirement for macro use, approved macros in Microsoft Office files in trusted locations can be allowed to execute.							R									17-Oct-15	15-Oct-15	Completed
P-16	The invoice simulation study will be done and the e-invoice will be sent after the controls are done through the system.			P				R									17-Apr-15	30-Mar-15	Completed

P-17	A control mechanism will be provided to ensure that the overwriting code works.							R									12-Feb-15	7-Feb-15	Completed
P-18	Uniforms of cleaning personnel will be provided in different colors.					R								P			6-May-15	30-Apr-15	Completed
P-19	Deputation matrix will be provided within the scope of meeting management.				P	R											3-Feb-15	3-Feb-15	Completed