DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

AN INFORMATION SECURITY RISK ASSESSMENT MODEL BASED ON BAYESIAN NETWORKS AND FUZZY INFERENCE SYSTEM

by

Sevilay BEKEN

August, 2019

İZMİR

AN INFORMATION SECURITY RISK ASSESSMENT MODEL BASED ON BAYESIAN NETWORKS AND FUZZY INFERENCE SYSTEM

A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of Dokuz Eylül University
In Partial Fulfillment of the Requirements for the Degree of Master of Science
in Department of Computer Science

by

Sevilay BEKEN

August, 2019

İZMİR

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"AN INFORMATION SECURITY RISK ASSESSMENT MODEL BASED ON BAYESIAN NETWORKS AND FUZZY INFERENCE SYSTEM"** completed by **SEVİLAY BEKEN** under supervision of **ASST. PROF. DR. METE EMİNAĞAOĞLU** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Mete EMİNAĞAOĞLU

Supervisor

Asst. Prof. Dr. Ayşe Öygü KINAY

(Jury Member)

Asst. Prof. Dr. Korhan KARABULUT

(Jury Member)

Prof.Dr. Kadriye ERTEKİN

Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGEMENTS

Foremost, I would like to express my sincere gratitude to my advisor Asst. Prof. Dr. Mete EMİNAĞAOĞLU for his continuous support, his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis.

Besides my advisor, I would like to thank Asst. Prof. Dr. Korhan KARABULUT and Asst. Prof. Dr. A. Övgü KINAY for their contribution to design process in my study. Also I would like to thank the experts and my colleagues in the company who helped me to gather data for analyzing process of my study.

Last but not the least, I would like to thank my family for their continuous encouragement throughout my years of study and through the process of researching and writing this thesis. Thank you.

Sevilay BEKEN

AN INFORMATION SECURITY RISK ASSESSMENT MODEL BASED ON BAYESIAN NETWORKS AND FUZZY INFERENCE SYSTEM

ABSTRACT

This study proposes an information security risk assessment model for calculating both qualitative and/or quantitative risk factors by using Bayesian network model and fuzzy inference system. The proposed model is developed for a software services company in order to evaluate the information security risks according to their test processes. First of all, in order to collect data for our risk assessment model, information assets, vulnerabilities, threats, and related risk values are identified and analysed with experts and managers based on the testing process in the company. The relations between identified and selected threats, vulnerabilities and information risks constructed in the Bayesian network. This Bayesian model is used for calculation of marginal probabilities for each risk factor. After completing the construction of Bayesian network, several fuzzy membership functions are designed for assets' values, relative risk values and risks' probabilities. Then, Fuzzy decision rules are constructed and derived for some of the chosen risks by using the assets' values, relevant risk probabilities, and relative risk values. Lastly, aggregation and defuzzification process are completed for calculating the impacts of risk values.

Keywords: Information security management, risk assessment, Bayesian networks, fuzzy inference system

BAYES AĞLARI VE BULANIK ÇIKARIM SİSTEMİ TABANLI BİR BİLGİ GÜVENLİĞİ RİSK DEĞERLENDİRME MODELİ

ÖZ

Bu çalışmada, nitel ve/veya nicel bilgi güvenliği risk unsurlarını saptamak ve analiz etmek amacıyla Bayes ağı modeli ve bulanık çıkarım sistemi kullanılarak bir bilgi güvenliği risk analiz modeli sunulmaktadır. Önerilen model, bir yazılım şirketinin bilgi güvenliği unsurlarını değerlendirmek üzere şirketin test süreçleri kapsamında geliştirilmiştir. Risk değerlendirme modeli için öncelikle veri elde etmek amacıyla, bilgi varlıkları, zafiyetler, tehdit unsurları ve ilgili risk faktörleri şirketteki uzman ve yöneticiler ile beraber test süreçleri kapsamında değerlendirilmiş ve analiz edilmiştir. Saptanan tehdit, zafiyet ve risk unsurlarının birbirleri ile olan ilişkileri Bayes ağı modeli kullanılarak oluşturulmuştur. Bu Bayes ağı her bir risk faktörünün bileşen olasılıklarının hesaplanmasında kullanılmıştır. Bayes ağının oluşturulması tamamlandıktan sonra, bilgi varlıkların değerleri, göreceli risk değerleri ve risklerin olasılıkları için bulanık üyelik fonksiyonları tasarlanmıştır. Ardından, bulanık karar kuralları bilgi varlıkların değerleri, risklerin olasılıkları ve göreceli risk değerleri kullanılarak oluşturulmuştur. Son olarak, oluşturulan bulanık çıkarım sistemi ile risklerin etki değerleri hesaplanmıştır.

Anahtar Kelimeler: Bilgi güvenliği yönetimi, risk değerlendirmesi, Bayes ağları, bulanık çıkarım sistemi

CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

CHAPTER ONE
INTRODUCTION

Information becomes the most essential asset for all companies and because of this reason; information security has become an important concern in companies based on their size and complexity. Information security can be defined as the protection of data or information to prevent loss, unauthorized access, modification, or misuse. Companies should ensure that systems and applications operate effectively while protecting information with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

The fundamental objectives of information security are confidentiality, integrity, and availability. Each objective focuses on different part of protection for information. National Information Assurance (IA) Glossary (Committee on National Security Systems, 2010) defines confidentiality "as the property that information is not disclosed to system entities which can be users, processes or devices unless they have been authorized to access the information". Confidentiality is the property that data or information is not made available or disclosed to unauthorized people or processes. This factor aims the protection of information against unauthorized access, uses, and disclosures.

On the other side, integrity is "the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner" according to IA (Committee on National Security Systems, 2010). Integrity factor indicates that information must protect against unauthorized modifications or improper destruction. Within the scope of information security, appropriate backup in case of a threat, hazard, or natural disaster should be provided for integrity.

Lastly, according to the IA Glossary's definition (Committee on National Security Systems, 2010), availability is "the property that data or information is accessible and usable upon demand by an authorized entity". This factor indicates that authorized personal must be able to access the information. Especially doing backups in regular

basis is essential for sustaining availability in case of data loss due to a natural disaster or threat. Moreover, besides backup plans, disaster recovery and business continuity plans for business, governmental, educational, and etc. operations should be identified and planned in order to keep the organization operational.

To sustain confidentiality, integrity, and availability objectives of information security, risk assessment methodologies should be applied for the organization's operations. The information security risk assessment is a process of determining the security risks and problems, resolving security problems, and eliminating these risk factors to an acceptable level.

Risk assessment process has three key elements, which are asset, threat, and vulnerability elements. The assets are the main objects for organizations that need to be protected based on information security policies. Assets can be valuable information or resources such as computers, employees, internet connection and so on. According to ISO 27001 standard, threat is "potential causes of accidents that may cause harm to systems or organizations" and vulnerability is "the weak link of an asset that may be exposed by the threat" (ISO / IEC 27001, 2013). Determining assets, threats, vulnerabilities, risk values, and likelihood is critical for information strategy. Assets, vulnerabilities, threats, and risk factors should be identified, analysed, and controlled within the scope of security risk assessment process according to ISO 27005 standard (ISO / IEC 27005, 2011). The results retrieved from information security risk assessment process can give the managers the information they need to understand and by this way, the risks to their assets can be determined (Landoll, 2006). Determined risk factors can be ranked and prioritized by managers and necessary actions can be taken to reduce the risk factors.

This study aims to focus on constructing an information security risk assessment model correctly, efficiently, and effectively. In order to succeed this goal, in this study, both qualitative and quantitative risks are evaluated and calculated with a new information security risk assessment approach which is based on Bayesian network model and Fuzzy Inference System.

For information risk assessment process, combined methodologies are more useful than other methodologies when variability, uncertainty and subjectivity of the risk factors are considered. They allow to combine subjectivity and objectivity. Information risk factors can be modelled in Bayesian network model and risk probabilities can be calculated more accurately for business requirements with Bayesian network model. Hence, Bayesian network model is selected for this study. Additionally, to obtain more reliable and less subjective approach to the risk assessment process and to combine quantitative and/or qualitative risk factors, fuzzy inference system is used.

To the best of our knowledge, no similar model could be found in the literature that combines fuzzy operators or fuzzy inference methodologies with Bayesian network model about information security risk assessment methodologies. Hence, our model is different from other information security risk assessment models. In our study, GeNIe software is used for design and implementation of our Bayesian Network model. GeNIe is a tool that can be used to design and implement several Bayesian network models that calculates the conditional probabilities and marginal probabilities.

The proposed model is applied for a software services company according to their software test process. In our model, firstly the Bayesian network model was developed to analyse company's database security during the testing process. The assets, vulnerabilities, threats, risk factors and their relations were analysed with the experts and managers in the company. All risk and vulnerability factors were evaluated according to three main objectives of information security, which are confidentiality, integrity, and availability. After defining and analysing the assets, vulnerabilities, threats, risk factors and their relations in the system, experts' opinions were collected in order to sustain needful data for assets, threats, vulnerabilities, and risk probability values in the Bayesian network model.

After completing the Bayesian network model, fuzzy inference system was developed for risk management process. At last but not the least, risk factors were

evaluated within the information security risk assessment scope based on the results for information risk factors.

It should be stated that a simpler and different version of developed model was presented at an international conference (Beken & Eminağaoğlu, 2018). In that study, the Bayesian network model was developed for less risk factors, fuzzy inference system was constructed with less fuzzy decision rules, and all of the fuzzy membership functions were created manually without using MATLAB program. Results were also obtained manually. That model was used as a case study, maximum value for each of the risks were not calculated, and the final risk values and rankings were entirely different.

In the rest of this paper, information security risk assessment process, risk analysis methods for information security, Bayesian network model, and fuzzy inference system are introduced briefly in the literature review section. Then the proposed model explained and results are presented for selected company. The last section is the conclusion for evaluating the results according to final risk factors.

CHAPTER TWO
LITERATURE REVIEW

2.1 Information Security Risk Assessment

Due to fact that the structure of information technologies have become more complicated and the size of the data which organizations own are increasing exponentially, information security risk assessment has become essential for the organizations (Shamala et al., 2013). Hence, different methodologies and approaches have been developed for information security risk assessment. In this chapter, a brief summary of studies and different methodologies in information security risk management are presented.

M. C. Lee (2014) stated that "information security risk assessment process is the important prerequisite to achieve scientific and effective risk assessment". According to his work, "Information security risk assessment process includes following stages; preparation of risk assessment, asset identification, threat identification, vulnerability identification, and risk calculation" (Lee, 2014). Risk assessment process can be divided into six steps as follows (Fu & Xiao, 2012).

1) Determining assessment objects: This step includes defining the scope of the assessment. All valuable information or resources should be considered as assets for the system.
2) Choosing assessment methods and tools: Appropriate assessment methods and tools should be determined. Assessment process for selected method should be defined.
3) Risk identification: Especially considering the critical assets, their vulnerabilities and related risk factors should be identified.
4) Risk analysis: All determined risk factors should be analysed by combining the value of the assets, the likelihood and impact of the threats caused by vulnerabilities. After all, final results for risk values should be calculated.
5) Risk assessment: Results should be evaluated based on the experts' opinions and risk assessment report should be prepared. Risk assessment report includes the

study's purpose, the scope, selected risk assessment approach or model, and final results. Results generally shows observations for potential risk factors, vulnerabilities of the system, related threats, likelihood of risk values, and recommended actions or solutions.

6) Evaluation of risk factors: After risk assessment process, the prepared risk assessment results in order to control that risk factors and reduce risk values, risk control plans should be prepared and applied.

2.2 Information Security Risk Assessment Methods

Risk assessment and management are important parts of Information Security Management Systems. Huge changes in structure and type of information technologies have been done during the recent years. Hence, the necessity of information security and information security methodologies has increased for all organizations (Shamala et al., 2013). Due to this fact, for maintaining the information security, various risk management frameworks and methodologies have been conducted (Takçı et al., 2010). In this part related works about information security risk management models are summarized. Information security risk assessment methodologies can be categorized in three different groups as "qualitative", "quantitative" and "combined" methodologies. Both quantitative and qualitative risk analysis methods are included in the relevant standards such as ISO 27005 (ISO, 2011), ISO 27001 (ISO, 2013), and SP 800-30 rev. 1 (NIST, 2012).

Quantitative risk analysis methods are different from qualitative methods by "using mathematical and statistical tools to represent risk" (Karabacak & Soğukpınar, 2005). Quantitative Risk Analysis methods try to determine the value of risk by quantifying risk factors with two variables as monetary loss and time.

Qualitative security risk assessment methods use qualitative estimates while quantitative assessment methods use numerical estimates. Karabacak and Soğukpınar (2005) stated that "in qualitative risk analysis methods, risk is analysed with the help of adjectives instead of using mathematics". Qualitative risk analysis methods assign

levels for risk factors such as high, medium and low. These methods try to evaluate risk factors by personal and professional experience (Denys, 2006). In qualitative risk analysis, risk is analysed by the aid of subjective qualitative scalar values and methods. Compared to quantitative methodologies, qualitative methods are easier to apply. Also, they allow to determine the highest risk values in short time. Besides their advantages, qualitative methods have some disadvantages as not determining the results using numerical measures and results obtained with approximates (Lee, 2014). Wawrzyniak (2006) stated that "qualitative methods do not offer enough information output to be useful tools for the risk management process". Qualitative methods are evaluated as more comprehensive and simpler than quantitative methods. On the other hand, risk identification process is subjective; the model is established based on information security experts' opinions (Aslam et al., 2017).

Li et al. (2017) compared the qualitative and quantitative risk assessment methods in their study and they have stated that; "Qualitative assessment methods are the earliest and most widely applied methods in the risk assessment process. They use qualitative indicators to assess risks, and the results are often expressed as a qualitative risk level. These methods are more comprehensive, in-depth, and simple under certain circumstances. … In contrast, quantitative risk assessment methods adopt specific quantitative indicators to conduct risk assessment, and the results are often in forms of specific risk values. Compared with qualitative methods, quantitative methods are more intuitive and reasonable."

Some of the quantitative security risk analysis methods are "risk value, annual loss expectancy, safeguard value, and return of investment" (Fu & Xiao, 2012). The most common and most frequently used quantitative method of risk assessment is Annual Loss Expectancy (ALE) model. ALE model is "based on the idea of expected loss, which is the product of probability of occurrence of events which have negative impact on IT and values of caused by them losses" (Fu & Xiao, 2012). Parameters used within the scope of Annual Loss Expectancy method are briefly described as follows (Yuhan et al., 2013).

Exposure Factor (EF) stands for the percentage of the loss when an asset is effected by a threat.

Asset Value (AV) is monetary value of the asset.

Single Loss Expectancy (SLE) is monetary loss derived from the occurrence of a specific event.

Annualized Rate of Occurrence (ARO) is used for approximate frequency of a threat occurs in a year.

Annualized Loss Expectancy (ALE) is described as "annual expected financial loss caused by the occurrence of a specific event" (Yuhan et al., 2013). The ALE approach is based on calculating the loss expectation and multiplying the possibility of loss for each attack over a period. The formulas for ALE method is presented as follows.

$$SLE = AV \; x \; EF \tag{2.1}$$

$$ALE = SLE \; x \; ARO \; x \; ALE \tag{2.2}$$

$$ALE = \sum_{i=1}^{n} I(O_i)F_i \tag{2.3}$$

Where; $\{O_1, O_2, O_3 \ldots O_n\}$ is set of negative effects of event,
$I(O_i)$ is loss value resulting from event,
F_i is frequency of event i.

In 2005, Karabacak and Soğukpınar have proposed a new information security risk assessment method called ISRAM, which is "based on a quantitative approach that uses survey results to analyse information security risks". In their study, the aim of ISRAM model is explained as assessing the information risks caused by threats due to information security vulnerabilities. In order to succeed this goal, they analyse the information system by conducting a survey among the managers and related employees. The ISRAM method has seven steps and it is performed by using public opinion on the problem which sustained from the survey (Karabacak & Soğukpınar, 2005).

On the other hand, Karabacak and Soğukpınar (2005) claim that due to the fact that today's risk environment becomes more complicated and it has become hard to analyze with quantitative methods, qualitative methods are more useful for risk analysis.

Some of the qualitative methods are "fuzzy comprehensive evaluation method", "The Microsoft Corporate Security Group Risk Management Framework", and "CRAMM".

CRAMM stands for "CCTA risk analysis and management method". This method is a qualitative risk analysis tool developed by UK government's Central Computer and Telecommunications Agency in 1985 (Enterprise, 2005). CRAMM methodology consists of three stages. These stages are identify and value assets, identify threats and vulnerabilities and calculate risk factors.

In many studies, the fuzzy comprehensive evaluation method is used for qualitative risk assessment in information security (Long, Yong & Qianmu, 2008; Wu, Fu & Wang, 2009; Lee, 2014). Long, Yong & Qianmu (2008) have used fuzzy comprehensive assessment after establishing a system indicator in order to determine the security risk level of information system. In their study, they used four steps for the fuzzy comprehensive evaluation. First one is determining the information security risk factors and in their example analysis, they selected these factors as assets, threats, frangibility, and security measure which they gathered from the result after their Analytic Hierarchy Process. After that, they determined the sub-elements of those factors. In their example analysis, the sub-elements of the asset factor are secrecy, integrality, and usability. For the threat factor, sub-elements are condition factor and artificial factor. Finally, the sub-elements of security measure are Defendable safeguard and Protection safeguard. For each factor, a fuzzy matrix was established and moreover, all these factors were evaluated by the experts on the scale of five as "Higher, High, Moderate, Low and Lower". They get statistics of experts' judgments about all the factors in the system to calculate the main fuzzy matrix from single level results. In the fuzzy matrix among the results, the biggest value is evaluated. For the example analysis, since the risk value is found in the middle level, according to the

most subjection degree fundamental, the level of information security risk assessment is determined as the middle.

More details about Fuzzy Comprehensive Evaluation Method are given in section 2.4.

Moreover, there are other methods in the literature that use combined qualitative and quantitative methodologies. For instance, Analytic Hierarchy Process (AHP) method is a popular approach for in security risk assessment that use qualitative methodology combined with quantitative approach. In many studies AHP method seems to be preferred (Altuzarra, Moreno-Jimnez & Salvador, 2007; Award, Suitan, Ahmad, Ithnan & Beg, 2011).

In 2009, Wu, Fu & Wang have claimed that AHP Method is a useful multi-criteria decision technique which combines qualitative and quantitative components of the system in order to analyse, prioritize, and evaluate the alternative solutions. It's stated that "AHP can change from the qualitative index into quantitative index" (Award, Suitan, Ahmad, Ithnan & Beg, 2011). Hence, this method has been selected widely for information security risk assessment. Also, the analytic hierarchy process methodology has been used in various risk application areas such as "security policy decision making", "evaluating information security investments" and "security risk assessment" (Lee, 2014).

2.3 Bayesian Network

2.3.1 Conditional Probability

"The probability model is concerned with evaluating the likeliness of events" (Marmer, 2014, p.1). Though in some systems or models some prior information needs to be comprised (Marmer, 2014). In these cases, we need to measure the probability of an event to occur when another event has taken place or in other words we need to find the conditional probability when a certain event has happened. In other words,

conditional probability helps the calculation of the probability of a variable while it is depending on another variable (Bruner, 2019).

The definition of conditional probability is given as follows.

"Suppose that events A and B are defined on the same probability space, and the event B is such that $P(B) > 0$. The conditional probability of A given that B has occurred is given as follows." (Marmer, 2014, p.1).

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \tag{2.4}$$

2.3.2 Marginal Probability

The marginal probability distribution is defined as "the distribution of the subset of the random variable in the theory of probability" (The Marginal Probability Functions, 2019). With the help of marginal probability, we can calculate the probability of occurrence of an event without the other events' values. Bruner stated, "The marginal probability is the probability of occurrence of a single event. In calculating marginal probabilities, we disregard any secondary variable calculation."

This type of distribution has been named as marginal because these are in the margins of a probability distribution table and also the marginal probabilities are calculated as summing values in the probability distribution table throughout rows or columns. (Glen, 2014). In order to calculate marginal distributions, there are some rules that need to be sustained such as, "data has to be bivariate" and "you are only interested in one of the random variables" (Glen, 2014). The definition and the calculation of marginal distribution are given below.

If X and Y are discrete random variables and $f(x,y)$ is the value of their joint probability distribution at (x,y), the marginal distributions of X and Y are shown below (Glen, 2014).

$$g(x) = \Sigma y\, f(x,y) \tag{2.5}$$

$$h(y) = \Sigma x\, f(x,y) \tag{2.6}$$

2.3.3 Bayes' Theorem

Bayes' theorem is a formula to describe the conditional probability relationships between variables (Wang, Fan, Mo & Xu, 2016). Bayesian theorem is used for calculating the possibility of an event to occur when we know the probability of related event.

The equation of Bayes' theorem is given in (2.2). In this equation, A and B denote the events; *P (A | B)* denotes the conditional probability that calculates the likelihood of A given that B is true. Similarly, *P (B | A)* represents the probability of B when A is known to have occurred.

$$P(A|B) = \frac{P(B|A).P(A)}{P(B)} \tag{2.7}$$

For our model, with the help of Bayes' theorem we can calculate the possibilities of an information risk to occur when we know the probabilities of related threats and vulnerabilities'. Since calculation of the risks' probabilities are needed, we will use Bayes' theorem for getting the risk probability by using the related threats' possibilities. For instance in our Bayesian network model, which will be explained in design and implementation section, we calculate the probability of risk "Unauthorized Change or Damage of Data" to occur when we know the probabilities of related two threats "Resignation Or Expel With Client Data" and "Hackers/Cyber Criminals" and related five vulnerabilities "Computers Vulnerable To Unauthorized Access", "VPN Connection Vulnerable To Unauthorized Access", "Disgruntled IT Users" "Disgruntled Test Users" and "Disgruntled Test Support Users" by using Bayes' theorem.

2.3.4 Bayesian Network Model

A Bayesian network is a graphical model that encodes the joint probability distribution for a set of random variables. A Bayesian network is a way of describing the relationships between causes and effects, and contains nodes and arcs. Bayesian network models are widely used in data mining, machine learning, and artificial intelligence. With the help of a Bayesian network model, the problems, causes of those problems and all the relations between them can be modelled. When we have knowledge about probabilities of events, we are able to identify the possibilities of the problems. "A Bayesian network is a directed, acyclic graph whose nodes represent random variables and arcs represent direct dependencies" (Chin, Tang, Yang, Wong & Wang, 2009). Each connected node's conditional probability and the joint probabilities are calculated within the network. For instance, if event A is directly connected to B, and event B is directly connected to C, then the probability of observing three events' occurrence can be calculated by the joint probability *P(A,B,C)* as follows:

$$P(A, B, C) = P(C|A, B)P(B|A)P(A) \tag{2.8}$$

It should be noted that *P(A)* is the probability of event A, *P(B|A)* is the conditional probability that calculates the likelihood of B given that A is observed, and *P(C|A,B)* is the conditional probability that calculates the likelihood of observing C given that both A and B are true or has occurred.

There are three stages of constructing a Bayesian network model (Maglogiannis, Zafiropoulos, Platis & Lambrinoudakis, 2006). In their study they explained these stages as "determination of the variables and their relationships", "specifications of each variable states conditional probability, given the state of the parent variables" and "calculation the probabilities for all Network nodes according to the cause–effect relationships".

Bayesian network models are also used for network security solutions. Frigault, Wang, Singhal, and Jajodia (2008) have developed a model by using a dynamic Bayesian network model for measuring network security. They proposed "a dynamic Bayesian network based model to incorporate relevant temporal factors, such as the availability of exploit codes or patches, into attack graph-based security metrics" (Frigault, Wang, Singhal & Jajodia, 2008). Additionally, Bayesian network model has been used for Earthquake Risk Management and Cyber Security Risk assessment. Bayraktarlı, Ulfkjaer, Yazgan & Faber (2005) stated in their study that by using Bayesian network models, the uncertainties associated with all elements of an earthquake from the source mechanism, site effects, structural response, damage assessments and consequence assessment can be analysed.

It is stated that "Bayesian network has a strong advantage in dealing with issues of uncertainty" (Wang, Fan, Mo & Xu, 2016). Hence, Bayesian network models are useful for modelling today's complex and diverse information systems, some researchers proposed models that use Bayesian networks or dynamic Bayesian networks.

Wang, Fan, Mo, and Xu (2016) have used dynamic Bayesian network model for information security risk assessment. In their study, firstly they created a dynamic Bayesian network model and after this process, information system were analyzed and the probability of the risk was calculated. Lastly, they made experiments in order to analyze and compare the dynamic Bayesian network model with the static Bayesian network model (Wang, Fan, Mo & Xu, 2016).

2.4 Fuzzy Inference System

Fuzzy inference system is a qualitative method and "Fuzzy Comprehensive Evaluation Method" is one of the common qualitative methodologies for the information security risk assessment, which is based on the principle of fuzzy mathematics. This method has the principle of the fuzzy statistical methods through considering a combination of relative factors for evaluation to determine the weight of

various factors to make the evaluation of the pros and cons of the research objects (Yuhan et al., 2013).

Some of the advantages of fuzzy inference system are listed below.

- The number of necessary rules and decisions are less than other approaches.
- It's easier to evaluate more variables.
- Non-numerical values for variables are used and with this way, model gets closer to the real world.
- Designing a fuzzy inference model is easier than making conventional systems and that makes the cost of making fuzzy models lower. Also this advantage helps the system designer to create the preliminary model quickly without knowing the whole processes.
- This methodology simplifies knowledge acquisition and representation.
- Even few rules could encompass great complexity.

Besides its advantages, since fuzzy inference system has subjectivity factor and contains human judgments, some researches combine this methodology with other methods in order to create a model with less subjectivity and more accurately.

For information security risk assessment process, in 2005 Zhao, Wang, Wu & Ma have proposed a model based on fuzzy logic and entropy theory. In their work, they have constructed the hierarchy structure with analytic hierarchy process (AHP) method and they used fuzzy logic for calculation of the risk degree due to the uncertainty of risk factors. After that, they used entropy theory to determine and ensure the weight vector of the risk factors. They stated that the method of entropy-weight coefficient were applied in order to overcome the subjectivity factor (Zhao, Wang, Wu & Ma, 2005).

Long, Yong & Qianmu used an approach that combines analytic hierarchy process and fuzzy comprehensive method in their study (2008). They claimed that their model which is a combination of AHP and fuzzy comprehensive method, "solves the difficulty of the qualitative index and quantitative evaluation in the risk assessment

process” (Long, Yong & Qianmu, 2008). They have shown an example of information risk assessment of a university site based on their approach. In 2014, Lee reviewed AHP model, neural networks, fuzzy logic, group decision making, software computing and hybrid models in the frame of information security risk problems. He stated that the application areas include “information security risk analysis”, “information security risk assessment”, and “information security management”. In his research, he also stated that to improve performance of AHP method, Fuzzy Comprehensive evaluation method can be used for reduction the feature subset (Lee, 2014).

CHAPTER THREE
PROPOSED MODEL

The proposed model was firstly developed for a software services company, whose main business activity is software testing, in order to evaluate the information security risk factors during their critical business processes. Their main business processes are based on software testing procedures and systems. Company's customers are generally in the telecommunication sector. The company has seventy employees and sixty-four of them are working in software testing projects. The working place layout is an open-office type.

First of all, the Bayesian network model was designed based on the testing process in the selected company. Secondly, fuzzy membership functions were constructed for both assets and risk factors. At last but not the least, after these steps, risk factors were evaluated within the information security risk assessment scope based on the results for information risk factors. Details about the implemented approach were explained in the Design and Implementation section.

The flow chart for the steps of our proposed model is given in Figure 3.1. As can be seen in the flowchart, first step of our model is the construction of the Bayesian network model. Primarily, the information assets, vulnerability elements, threat values and risk values were determined for the system. In order to determine these information assessment elements, the company's software testing processes were analysed with the experts in the company. All related information risk values, threats, vulnerabilities and the relations among them were identified and Bayesian network model was constructed according to the relations. Then, all of these information elements' values are gathered from experts' opinions and the vulnerability, threat and risk values were used in the constructed Bayesian network model to sustain the marginal probabilities of risk values. The details about the process of data collection are explained in materials section.

For fuzzy inference system, first of all the fuzzy membership functions were constructed for both risk probabilities and asset values. While the Gaussian fuzzy membership function is used for information risk values, trapezoidal fuzzy membership function is selected for both assets values. After construction of all fuzzy membership functions, fuzzification rules were determined. Then, the marginal probability values of information risks which were gathered previously from the Bayesian network model, were used for the fuzzification process in the fuzzy inference system. Fuzzification process was also applied for asset values to get fuzzy asset values. Then, fuzzy rules were derived and activated for obtained values for risks and assets' fuzzy values. After that, aggregation and defuzzification process were applied in order to get risk output values. These risk values were ranked so as to compare risk values and report them to the company. The details about design and implementation process of the model is explained and detailed in the design and implementation section. At the end of this process, the company is able to analyse these risk values and they can find solutions for reducing and eliminating these risk factors starting from the highest risk value. Final results for the company's selected system and their processes, are shown in the results section.

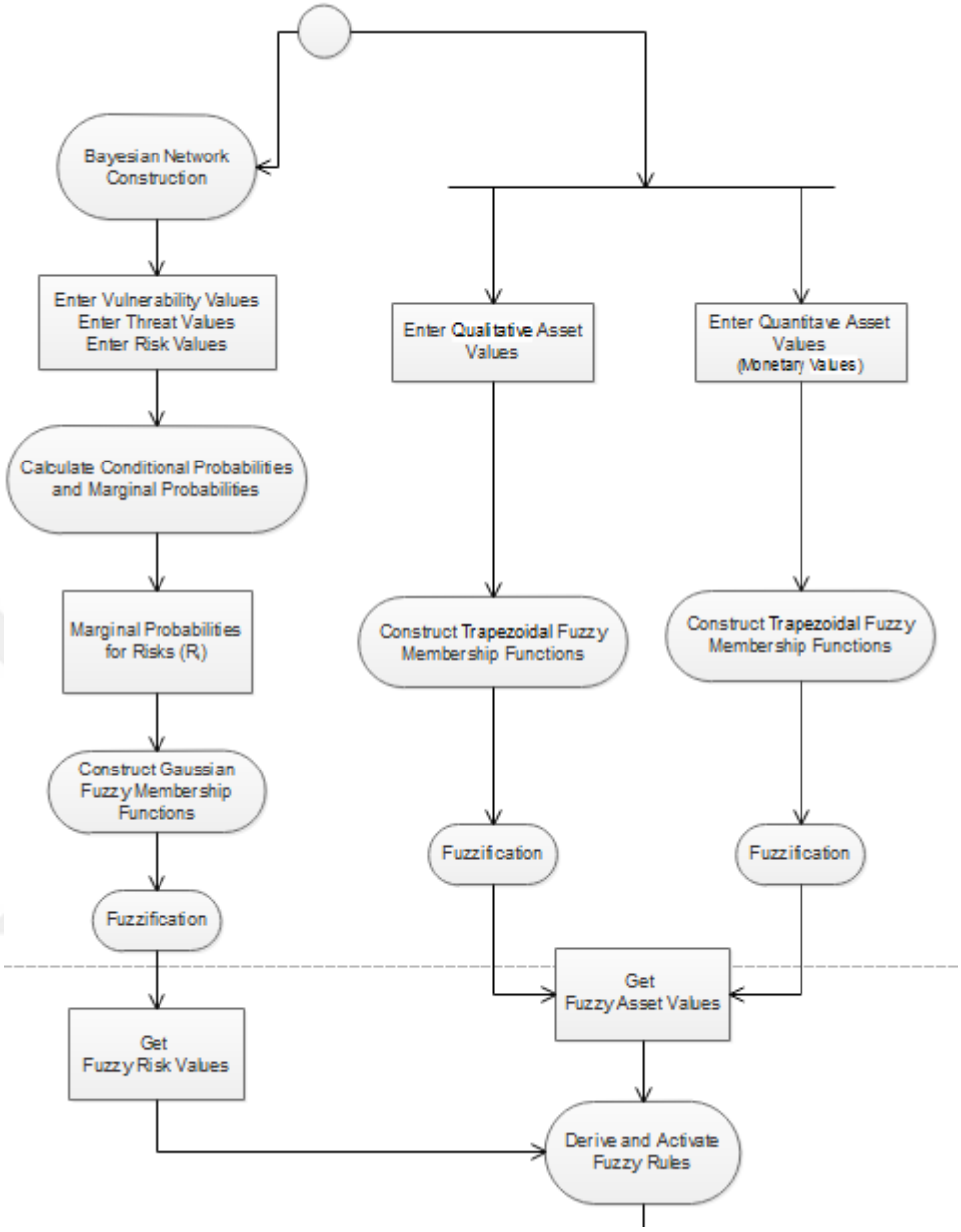


Figure 3.1 Flowchart for proposed model

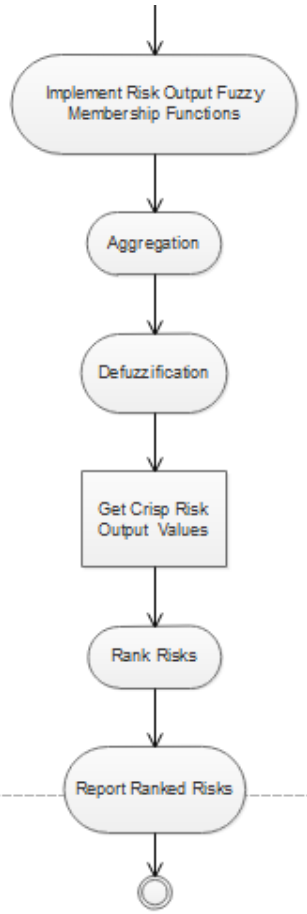


Figure 3.1 continues

3.1 Materials

In order to collect expert opinions about probabilities in the Bayesian network model, questions about threats, risks, and assets were asked to the experts in the company. Fifty-one experts who knows the company's testing process very well and are responsible for company's software test process contributed for analysing the system. The system was analysed based on four main categories and the questions while analysing these categories are explained in below.

- Assets – what do we have?
- Vulnerabilities – is the asset at risk?

- Threats – what / who will attack / damage / destroy it?
- Risk factors – what are the main risks?

Experts' opinions about the company's testing process were collected based on these categories and questions. The final elements of our risk assessment process are listed below. These information assets, vulnerabilities, threats, and risk elements were used in the scope of risk assessment process.

1. Seven assets: "Data stored in Computers/Laptops", "VPN Connection", "Customer data stored in database", "Test data", "IT Users", "Test Users", and "Test Support Users".

2. Twelve vulnerabilities: "Computers Vulnerable to Malfunctions", "VPN Connection Vulnerable to Malfunctions", "Vulnerable to Physical Problems/Damages", "Vulnerable to Malicious Codes", "Might Be Easily Lost/Stolen", "Lack of Experience or Training", "Lack of Awareness", "Computers Vulnerable to Unauthorized Access", "VPN Connection Vulnerable to Unauthorized Access", "Disgruntled IT Users", "Disgruntled Test Users", and "Disgruntled Test Support Users".

3. Eleven threats: "Technical Problems", "Malicious Code", "Blackout/Brownout", "Fire", "Earthquake", "Thieves", "Human Error/ Failure by IT Users", "Human Error/Failure by Test Users", "Human Error/ Failure by Test Support Users", "Hackers/Cyber Criminals", and "Resignation or Expel with Client Data".

4. Nine risks: "Unavailability of Computers", "Network Connection Loss", "Loss of Test Data", "Database Crash", "Disclosure of Confidential Information", "Unauthorized Change or Damage of Data", "Discontinuation of Testing Processes", "Inaccurate Test Results", "Prestige Loss".

For the information security assessment process all the above elements were evaluated in the frame of below questions based on experts' opinions and their previous experience in the company. Twenty-one questions were prepared to define the possibilities of threats in the system. Three different levels (Low, Medium, and High) of scale were used in this phase. In order to analyse risk values, thirty-four questions were asked to the experts and the answers were evaluated by using a scale with five levels (Very Low, Low, Medium, High, and Very High). And finally, experts were asked to evaluate seven different information assets based on either their approximate monetary values or a scale of ten points (one, two … ten) where "one" represents the lowest value, "ten" represents the highest value. Hence, in order to get experts' opinions, information security evaluation form is prepared. A partial view of the prepared form for threat values is given in Table 3.1 and the evaluation form for the asset values is given in Table 3.2. The full version of the prepared information security evaluation form is given in Appendix 1. An example of the evaluation form which was filled by an expert from the company is given in Appendix 2.

Table 3.1 The information security evaluation form for the threat values

	L	**M**	**H**
Due to technical problems, what is the possibility of a breakdown of your computer?			
Due to technical problems, what is the possibility of a VPN connection loss occurs?			
For your work process, what is the negative impact level of an earthquake happens?			
What is the possibility of Malicious Codes cause a database crash?			

Table 3.2 The information security evaluation form for the asset values

Assets	The Scale of Ten 1: The Lowest; 10: The Highest	Monetary Value (TL)
Data stored in computers/laptops		
IT users (experience / knowledge)		
Customer data stored in Database		
Test data		
VPN connection		
Test users (experience / knowledge)		
Test support users (experience / knowledge)		

All these forms were used for evaluating the asset values and also the possibilities of threats and risks to get experts' opinions. Collected data was analysed for calculating the probability of related threat, risk and asset values. For each question and its corresponding criticality, the average scores were calculated based on the answers of experts. All of these average values were used in the Bayesian network model to calculate the conditional probabilities of the related threat and risk. Table 3.3 shows the average values for evaluated assets. All the experts preferred to evaluate assets' values on the scale of ten so the average values are calculated for getting the final values for assets. These asset values will be used in the next step of our model which is the fuzzy inference system.

Table 3.3 Asset values evaluated by experts' evaluations

Asset name	Asset value
Data stored in computers/laptops	6.90
IT users (experience / knowledge)	7.74
Customer data stored in Database	7.55
Test data	7.21
VPN connection	8.40
Test users (experience / knowledge)	8.20
Test support users (experience / knowledge)	8.01

Additionally, after all assets, vulnerabilities, threats and risk values are selected with experts in the company, these are reviewed by two different information security experts from outside of the company in order to analyse the system from a different

perspective. Based on their review, two additional risk elements are added to the Bayesian network model. These risks are; “Loss of Workforce”, and “Penalty or Legal Issues”. For evaluating these additional risk elements, experts in the company were consulted to get their opinions. They evaluated these risk elements by using the same scale with five levels. Consequently, eleven risk values are selected and evaluated for the next steps of our study.

3.2 Design and Implementation

After determining the information assets, vulnerability elements, threat values and risk values for the system with the help of the experts in the company and also information security experts, all related information risk values, threats, vulnerabilities and the relations among them were identified and Bayesian network model was constructed according to their relations in order to calculate and retrieve the probabilities of each of information security risks in our model. The model was constructed in GeNIe software (GeNIe Modeler, 2018). The entire Bayesian network model is shown in the Figure 3.2.

In the GeNIe model, vulnerability values are notated in blue color, threats are shown in orange color and risk values are shown in yellow color for visual convenience. After collection of data, vulnerability values, threats and risk factors are evaluated one by one. Conditional and marginal probabilities are calculated in the GeNIe software according to marginal probability distribution.

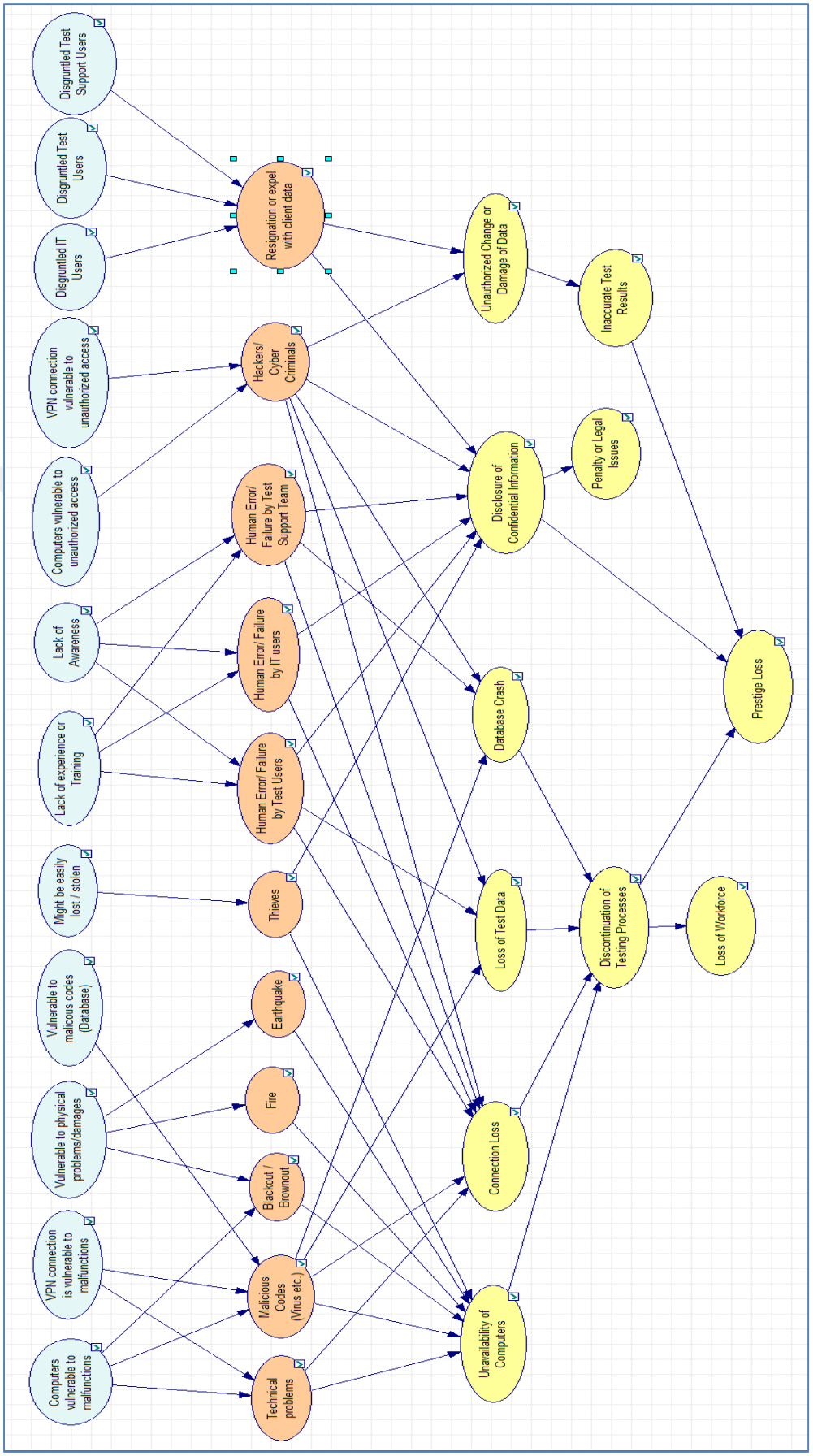


Figure 3.2 Entire Bayesian network model

A small excerpt from the Bayesian network model used in this study is denoted in Figure 3.3.

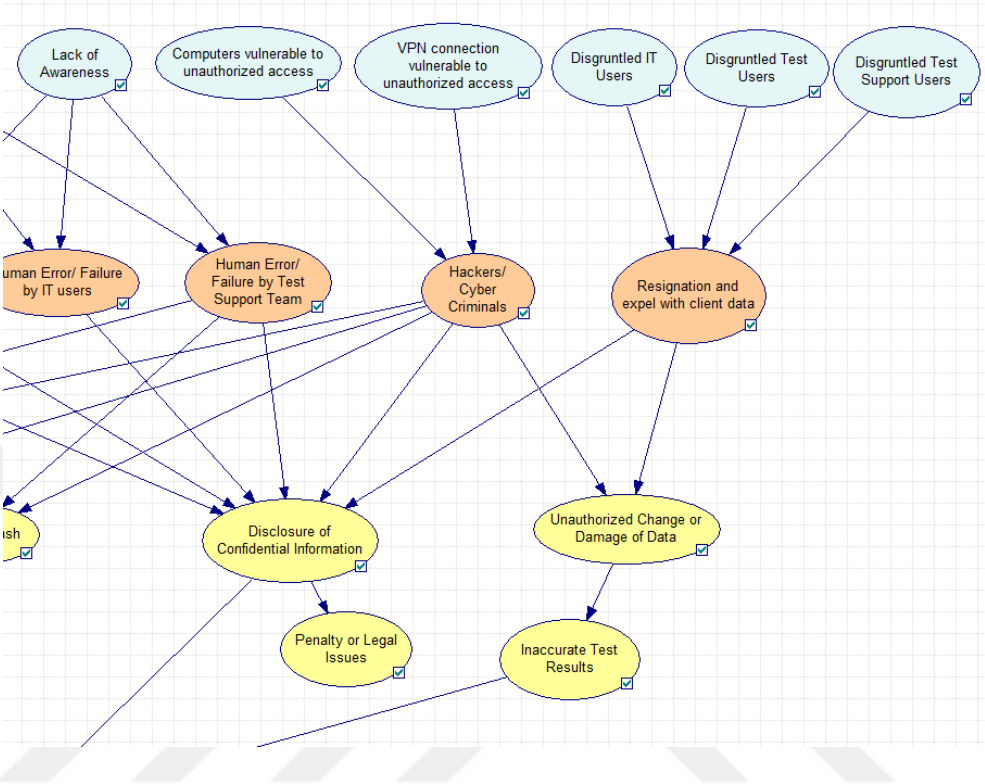


Figure 3.3 A partial view of the Bayesian network model

After collecting experts' opinions, we calculated average values of all threat and risk values. The results for threat eleven for example is shown in Table 3.4.

Table 3.4 Results based on experts' evaluation for threat eleven "resignation or expel with client data"

	Probability For 'Resignation and Expel with Client Data'			
	Low	**Medium**	**High**	**Total**
Disgruntled IT Users	0.490	0.255	0.255	1.00
Disgruntled Test Users	0.529	0.314	0.157	1.00
Disgruntled Test Support Users	0.490	0.412	0.098	1.00
Average	0.503	0.327	0.170	**1.00**

In order to use in the constructed Bayesian network model, we need to know all probabilities for related information security elements. In the Bayesian network model calculation of the marginal probability of a risk value is based on the values of all threats' probabilities related to that risk value. In a similar manner, marginal probability of a threat value is calculated according to the all vulnerability probabilities related to that threat value. For this purpose, we categorized the vulnerability and threat probabilities. For instance, the categorization of vulnerability probabilities for threat eleven "Resignation or expel with client data" is shown in Table 3.5. In the table the values represent the vulnerability probabilities. For this threat value, it can be seen in the constructed Bayesian network model that this threat is related to three vulnerabilities; "Disgruntled IT Users", "Disgruntled Test Users" and "Disgruntled Test Support Users". These relations in Bayesian network model was denoted in Figure 3.4. Categorization is applied based on the different vulnerability values as "yes" or "no". It should be noted that for a vulnerability factor, the sum of the two probabilities of that vulnerability exists or not (yes or no probabilities) equals to one. Since the threat "Resignation or expel with client data" has three related vulnerabilities, four categories are defined for different vulnerability probability values. Category one shows when the probability of "Disgruntled IT Users", "Disgruntled Test Users" and "Disgruntled Test Support Users" are all marked as yes. Category two shows when one of the vulnerability probability is marked as no, the others are marked as yes. Category three shows when the two of the vulnerability probabilities are marked as no, the other one marked as yes. The last category shows when all the vulnerability probabilities are all marked as no. Categorization process is done for all threat and risk values in the Bayesian network model.

Table 3.5 Categorization for threat eleven "resignation or expel with client data"

Vulnerability Probabilities											
Category 1			**Category 2**								
IT	**Test**	**TestSup**	**IT**	**Test**	**TestSup**	**IT**	**Test**	**TestSup**	**IT**	**Test**	**TestSup**
yes	yes	yes	yes	yes	no	yes	no	yes	No	yes	yes
0.25	0.35	0.30	0.25	0.35	0.70	0.25	0.65	0.30	0.75	0.35	0.30
Category 3									**Category 4**		
IT	**Test**	**TestSup**	**IT**	**Test**	**TestSup**	**IT**	**Test**	**TestSup**	**IT**	**Test**	**TestSup**
yes	no	no	no	yes	no	no	no	yes	No	no	no
0.25	0.65	0.70	0.75	0.35	0.70	0.75	0.65	0.30	0.75	0.65	0.70

For all these categories, weighting factors are given to different levels (low, medium and high). Then, we multiplied these weighting factors by the average values which were gathered previously from experts' opinions for related information security factor. Since sum of these values are not equal to one, we used normalization for getting the final values to use in the Bayesian network model as input. In Table 3.6 whole process of getting the final values to use in the Bayesian network model for threat eleven "Resignation or Expel with Client Data" is shown. In this table WF means the weighting factor and AV represents average value.

Table 3.6 Normalization process for threat eleven "resignation or expel with client data"

Threat Level	**Average Values**	**WF for C1**	**AV*WF**	**cumul.normalize (Sigma=1)**	**WF for C2**	**AV*WF**	**cumul.normalize (Sigma=1)**
L	0.503	0.10	0.05	0.21	0.10	0.05	0.20
M	0.327	0.20	0.07	0.29	0.30	0.10	0.40
H	0.170	0.70	0.12	0.50	0.60	0.10	0.40
Total	1.00	1	0.23	1.00	1.00	0.25	1.00

Threat Level	**Average Values**	**WF for C3**	**AV*WF**	**cumul.normalize (Sigma=1)**	**WF for C4**	**AV*WF**	**cumul.normalize (Sigma=1)**
L	0.503	0.35	0.18	0.51	0.80	0.40	0.87
M	0.327	0.40	0.13	0.37	0.15	0.05	0.11
H	0.170	0.25	0.04	0.11	0.05	0.01	0.02
Total	1.00	1.00	0.35	1.00	1.00	0.46	1.00

After entering all probability values which were gathered from normalization process, marginal probability values of all risk elements are calculated in the GeNIe program. We need this data for the next step of our model which is fuzzy inference system.

The marginal probabilities for the threat “Resignation or Expel with Client Data” are denoted in Figure 3.4. Also the categorization and normalization processes are completed for all risk factors and the marginal probabilities are calculated in the GeNle program. For instance, the marginal probability values for the risk “Inaccurate Test Results” were calculated in GeNle program as can be seen in Figure 3.5.

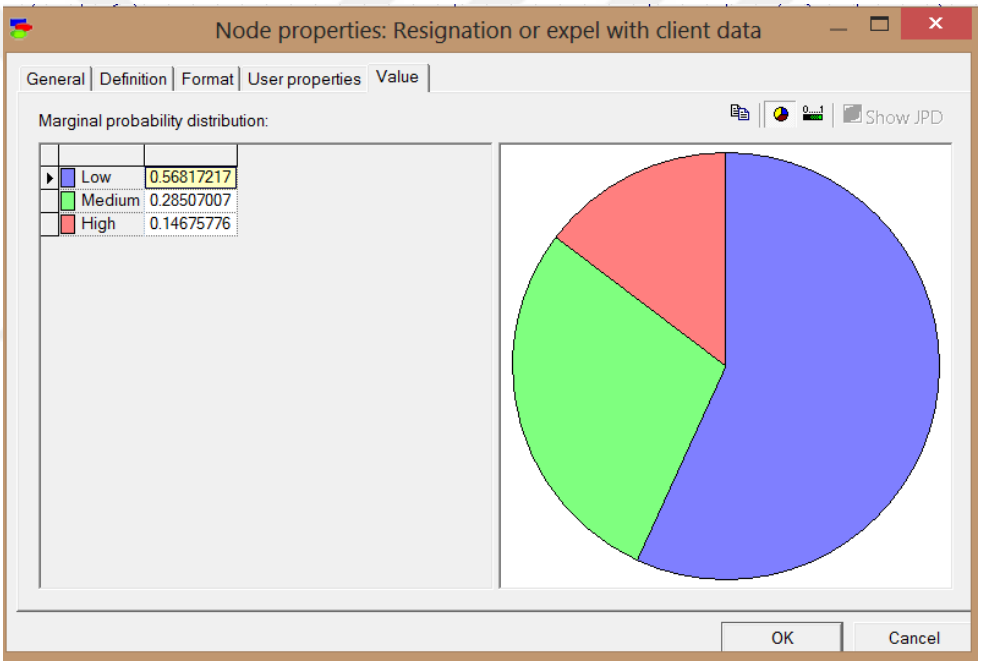


Figure 3.4 Marginal probabilities for the threat “resignation or expel with client data"

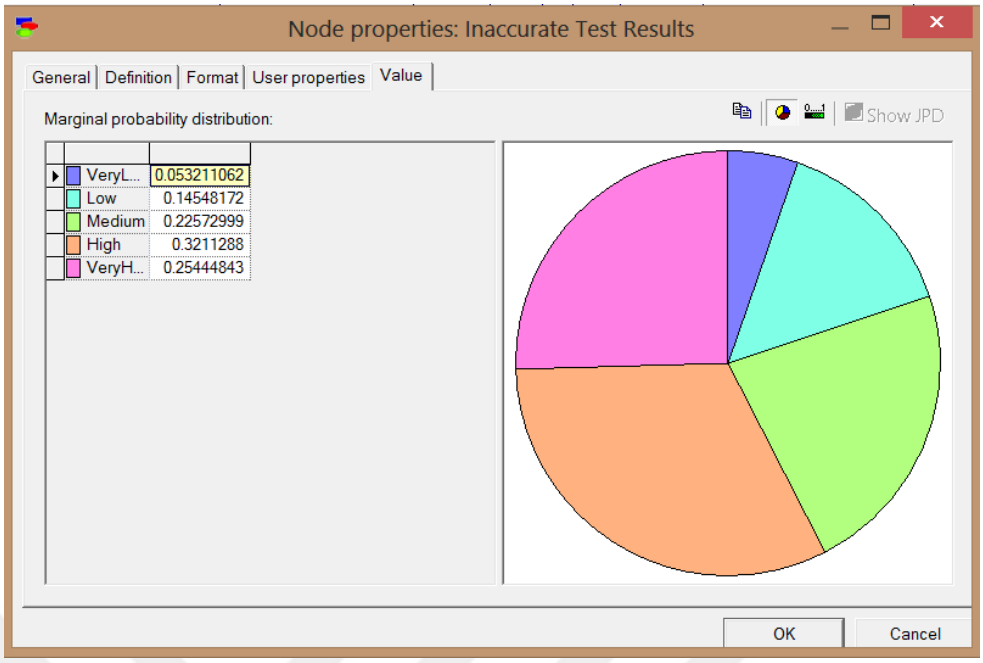


Figure 3.5 Marginal probabilities for the risk "inaccurate test results"

After calculating all marginal probability values, we have evaluated all risk elements and used normalization process for getting the final probability values for all risk elements. Normalization process is needed in order to compare data more easily among the risk values. In our study we used max-min normalization process and it is computed based on formula 3.1. Normalized values of marginal probabilities for all risk values are shown in Table 3.7.

$$z_i = \frac{x_i - \min(x)}{\max(x) - \min(x)} \tag{3.1}$$

Table 3.7 Normalization process and normalized values of marginal probabilities for all risk

Risk_ID	Level	Marginal Probability	Min-max Normalized Marginal Prob.
R1	vL	0,138	0,308
R1	vH	0,164	0,366
R1	L	0,195	0,436
R1	M	0,238	0,530
R1	H	0,265	0,590
R2	vH	0,088	0,197
R2	vL	0,134	0,298
R2	L	0,228	0,509
R2	M	0,261	0,583
R2	H	0,288	0,643
R3	vH	0,148	0,330
R3	vL	0,162	0,362
R3	L	0,213	0,474
R3	M	0,226	0,505
R3	H	0,251	0,559
R4	vH	0,074	0,164
R4	vL	0,144	0,320
R4	H	0,244	0,544
R4	L	0,267	0,594
R4	M	0,272	0,607
R5	vH	0,132	0,294
R5	M	0,189	0,422
R5	vL	0,192	0,429
R5	L	0,235	0,524
R5	H	0,252	0,561
R6	vH	0,131	0,292
R6	vL	0,169	0,377
R6	H	0,171	0,381
R6	L	0,18	0,401
R6	M	0,349	0,778
R7	vL	0,074	0,164
R7	L	0,098	0,219
R7	M	0,201	0,448
R7	vH	0,269	0,601
R7	H	0,358	0,798
R8	vL	0,053	0,119
R8	L	0,145	0,324
R8	M	0,226	0,503
R8	vH	0,254	0,567
R8	H	0,321	0,716
R9	vL	0,026	0,058
R9	L	0,085	0,188
R9	M	0,137	0,305
R9	vH	0,375	0,835
R9	H	0,378	0,843
R10	vL	0	0
R10	L	0,019	0,043
R10	M	0,301	0,672
R10	H	0,417	0,931
R10	vH	0,262	0,583
R11	vL	0,041	0,09
R11	L	0,06	0,133
R11	M	0,114	0,253
R11	H	0,338	0,753
R11	vH	0,448	1

After normalization process, we evaluate normalized risk values of "very high" and "very low" scales for all risk values. Between these two values, the highest normalized value is selected for related risk element. For instance, seventh risk element's normalized values for very high and very low scales are "0.164" and "0.601"

respectively. Therefore, risk value for seventh risk element, which is "Discontinuation of Testing Processes", is assigned as "0.601" which is the highest value between very low and very high risk values. These process is completed for all risk elements and the final risk probability values for all risk elements are shown in Table 3.8.

Table 3.8 Final risk probability values obtained from Bayesian network model after normalization process

Risk No.	**Risk Name**	**Probability Value**
R1	Unavailability of Computers	0.366
R2	Connection Loss	0.298
R3	Loss of Test Data	0.362
R4	Database Crash	0.320
R5	Disclosure of Confidential Information	0.429
R6	Unauthorized Change or Damage of Data	0.377
R7	Discontinuation of Testing Processes	0.600
R8	Inaccurate Test Results	0.567
R9	Prestige Loss	0.835
R10	Loss of Workforce	0.583
R11	Penalty or Legal Issues	1

Because of the uncertainty of the risk factors, the fuzzy logic method, and a fuzzy inference system is used in this study. First, membership functions are determined for both assets and risk values. Hence, it could be deduced that membership function is a curve showing a point mapping points of inputting data into membership values, whose interval is between zero and one (Ariyanti et al., 2010).

Mamdani Fuzzy Inference System (FIS) was used for fuzzification, defuzzification, and aggregation operations in our risk assessment model. For each fuzzy rule, the minimum or maximum of the fuzzy membership values in the antecedent part is taken according to "and" or "or" operators in the antecedent part of that fuzzy rule. The membership value from operations on the predecessors / antecedents "truncates the membership function for the consequent or resultant part of that rule". This truncation or scaling is established for each rule, and then "the truncated membership functions from each rule are aggregated" (Ross, 2004). In order to create fuzzy membership function for assets and risk values, Trapezoidal membership function was selected and Gaussian membership function was used for risk probabilities. It should be noted that,

"the final risk / impact value" in our model represents the overall risk or impact that is produced as the outcome of the relevant asset value and that risk's probability value. Hence, the outcome of a fuzzy rule in our model gives the fuzzy risk value using Mamdani FIS. Using these membership functions and adjusting the parameters, the fuzzy membership values for crisp asset values, risk values, and risk probabilities are calculated. All of the fuzzy rules, membership functions, fuzzy operators and fuzzy calculations were developed, implemented and calculated by using MATLAB software (MATLAB, The MathWorks, Inc., 2018).

The formula for Trapezoidal membership function that is used for calculating asset values and risk values is shown as in equation 3.2.

$$\mu_F(x,a,b,c,d) = \begin{cases} 0, & if\ x < a \\ \frac{x-a}{x-b}, & if\ a \le x \le b \\ 1, & if\ b < x < c \\ \frac{d-x}{d-c}, & if\ c \le x \le d \\ 0, & if\ d < x \end{cases} \tag{3.2}$$

For Gaussian membership function which was used for risk probability values in our fuzzy inference system, the equation is shown in 3.3. This membership function is needed in order to derive the fuzzy values for marginal risk probabilities that are continuous values between 0 and 1. These probabilities were previously obtained from our Bayesian network model.

$$\mu(x,a,b) = e^{\frac{-(x-b)^2}{2a^2}} \tag{3.3}$$

Since all of the assets' values which we gathered from experts' opinions are above six points, fuzzy membership function for assets is designed for medium, high and very high values. "Very Low" and "Low" functions are canceled in the fuzzy membership function for asset values. The constructed membership functions in MATLAB program for asset values and risk probabilities are denoted in Figure 3.6 and Figure 3.7, respectively.

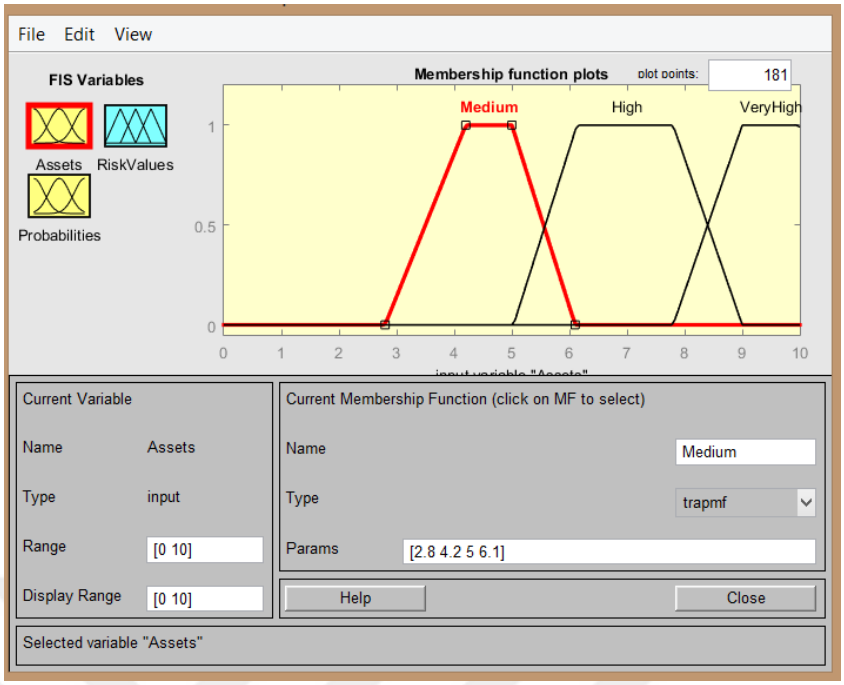


Figure 3.6 Trapezoidal membership function for asset values

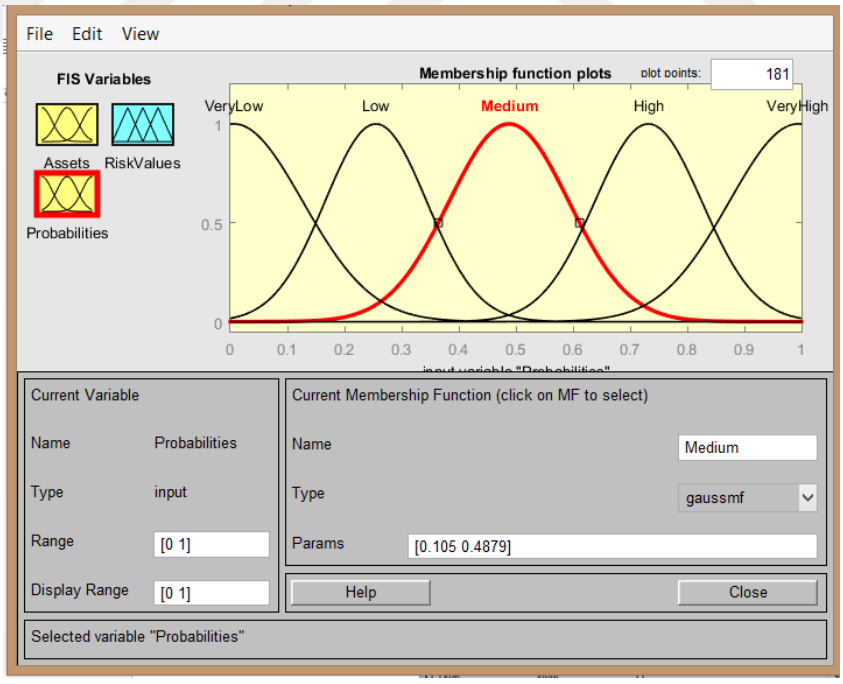


Figure 3.7 Gaussian membership function for risk probabilities

After defining fuzzy membership functions, sixteen fuzzy rules were constructed for the fuzzy inference process. For instance, suppose that a specific asset's crisp value

is given as 4, and the risk probability is calculated as 0.5 for a specific risk related with that asset. If we use the fourth fuzzy rule in our model *("If Asset is Low and Probability is Low, then Risk is Low"*), then according to Mamdani FIS, the antecedent part of this rule will give a fuzzy value as 0.411. This is achieved by finding the minimum of the fuzzy membership values (0.411 and 0.862) of asset and risk probability. All of the fuzzy decision rules were coded and executed in MATLAB and some of these rules are also denoted in Figure 3.8.

Aggregation was processed based on the fuzzy rules for each related risk. For calculating the crisp risk values during the defuzzification process, Center of Gravity method has been used. "If the output fuzzy set has at least two convex sub-regions, then the center of gravity (i.e., z^* is calculated using the centroid method) of the convex fuzzy sub-region with the largest area is used to obtain the defuzzified value z^* of the output" (Ross, 2004). This is given algebraically in equation 3.4.

$$z^* = \frac{\int \mu C_m(z) z dz}{\int \mu C_m(z) dz} \tag{3.4}$$

However, it should be noted that equation 3.4 is used when the membership values are continuous. If the values are discrete, the center of gravity method can be simply calculated as follows in equation 3.5.

$$z^* = \frac{\sum_{i=1}^{n} x_i \mu(x_i)}{\sum_{i=1}^{n} \mu(x_i)} \tag{3.5}$$

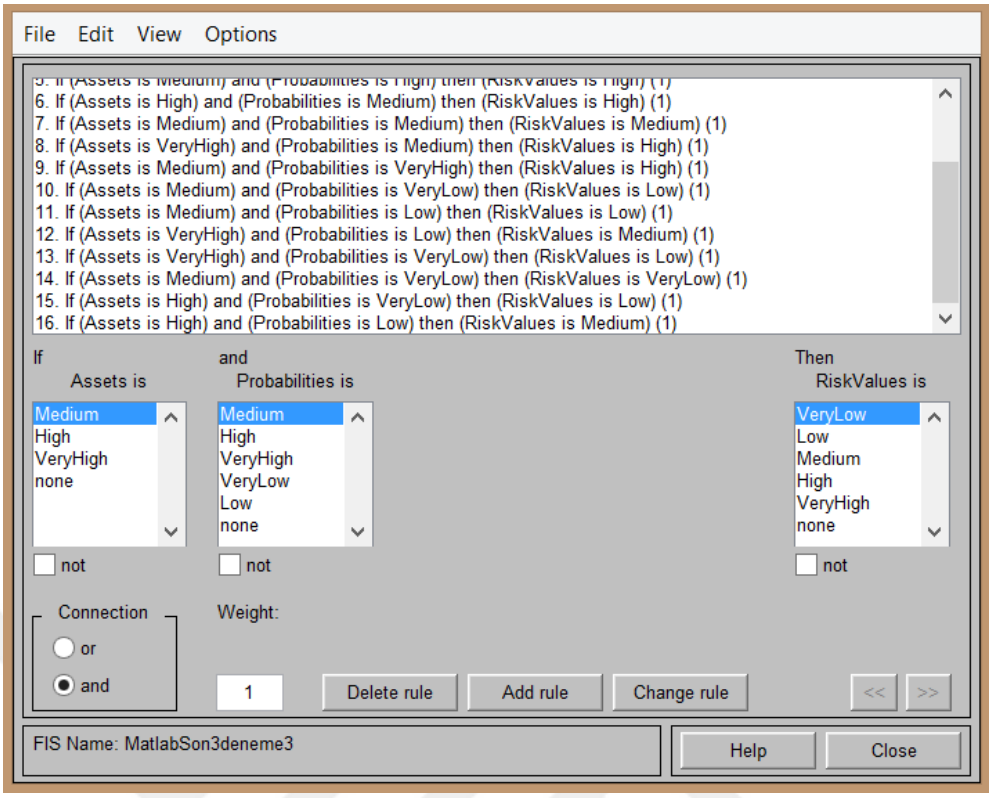


Figure 3.8 Some of the fuzzy decision rules used in our model

The defuzzification methodology can also be explained with a simple example. For instance, we can assume that a specific asset's crisp value is given as 5, and the risk probability is calculated as 0.73. Using the fuzzy membership tables in this study, and are aggregating all of the fuzzy rules mentioned in the previous page, then this risk's defuzzified value (by using the center of gravity method) can be calculated as follows:

$$R_d = \frac{(1x0.052)+(2x0.11)+(3x0.11)+(4x0.517)+\cdots+(8x0.617)+(9x0.167)+(10x0.167)}{(0.052+0.11+0.11+0.517+0.517+0.517+0.617+0.617+0.167+0.167)} = 7.99 \quad (3.6)$$

The abstraction of the entire fuzzy inference system that was implemented in MATLAB is also shown in Figure 3.9.

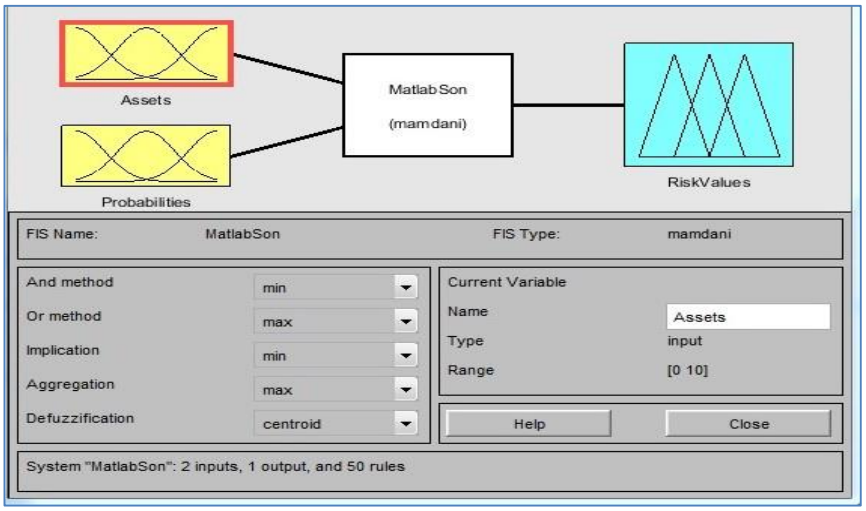


Figure 3.9 Abstraction of the entire fuzzy inference system in MATLAB

There were seven different assets within the scope of our information security risk assessment model and each of these were exposed to one or many risks. The relationship between assets and risks are denoted in Table 3.9. These relations are used in fuzzy inference system to identify which asset value and risk value should be entered for fuzzification process.

Table 3.9 Relationships between assets and risks

		RISKS										
ASSETS		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**	**R9**	**R10**	**R11**
A1	Data stored in Computers/Laptops	X					X		X	X		X
A2	IT Users	X		X		X	X	X		X	X	X
A3	Customer data stored in database				X	X				X		X
A4	Test data		X	X	X		X		X			
A5	VPN Connection	X	X				X			X		
A6	Test Users	X	X	X	X	X	X	X	X	X	X	X
A7	Test Support Users	X	X	X	X	X	X	X		X	X	X

3.3 Results

According to the methodologies and calculations that were described in previous sections, the model has been implemented and crisp risk values were obtained.

In the final part of our model, we used asset values and risk probability values for fuzzy inference system. The asset values were obtained by averaging the expert opinions' evaluation scores, which were described in materials section. These asset values were given as crisp inputs to the fuzzy inference system. The marginal probabilities of risks were calculated from the Bayesian network and they were explained in design and implementation section. These probabilities were also fed into the fuzzy inference system as the crisp input values. The fuzzy membership values of assets and risk probabilities were obtained by the membership functions. For each asset, relevant risk or risks were grouped, and then for each of these groups, all the fuzzy rules in the rule base were applied. Finally, aggregation and defuzzification operations were executed and risk / impact values were obtained. There were seven different assets that were exposed to one or many risks, which was mentioned in the previous section. Hence, there is a many-to-many relationship between the assets and risks which produces different defuzzified risk values. These different risk values corresponding to different assets are given in Table 3.10.

Table 3.10 Defuzzified risk values based on the relations between assets and risks

		Asset Values						
		A1	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**
Risk Values		6.9	7.74	7.55	7.21	8.4	8.2	8.01
R1	0.366	6.31	6.31	0	0	6.29	6.31	6.31
R2	0.298	0	5.30	0	5.30	5.48	5.38	5.32
R3	0.362	0	6.24	0	6.24	0	6.24	6.24
R4	0.320	0	0	5.55	5.55	0	5.62	5.55
R5	0.429	0	7.20	7.20	0	0	7.12	7.19
R6	0.377	6.51	6.51	0	6.51	6.41	6.51	6.51
R7	0.601	0	7.55	0	0	0	7.90	7.73
R8	0.567	7.54	0	0	7.54	0	7.73	0
R9	0.835	8.00	8.00	8.00	0	8.11	8.00	8.00
R10	0.583	0	7.54	0	0	0	7.81	7.70
R11	1	9.32	9.32	9.32	0	0	9.30	9.31

After calculating defuzzified risk values based on the relations between assets and risks, final evaluation of each risk with its unique value has been done. For sustaining the final value of a risk element, the highest risk value among its related assets' corresponding values has been selected and this process has been repeated for each of

the eleven risk elements. For instance, as it could be seen from Table 3.10, there exists four different defuzzified risk values for the second risk which are among the assets A4, A5, A6, and A7. The highest value for risk two belongs to asset A5, hence, the final risk value for second risk is 6.59. The final risk values were calculated by using this maximum operator and the risks were ranked according to this mechanism, which is given in Table 3.11.

Table 3.11 The final risk values

Risk number	Risk name	Final risk value
R11	Penalty or Legal Issues	9.32
R9	Prestige Loss	8.11
R7	Discontinuation of Testing Processes	7.90
R10	Loss of Workforce	7.81
R8	Inaccurate Test Results	7.73
R5	Disclosure of Confidential Information	7.20
R6	Unauthorized Change or Damage in Data	6.51
R1	Unavailability of computers	6.31
R3	Loss of Test Data	6.24
R4	Database Crash	5.62
R2	Network Connection Loss	5.48

It can be seen from Table 3.11 that the risk with highest score is “Penalty or Legal Issues” and the risk with the lowest value is “Network Connection Loss”. These results were also cross-checked and approved by the experts in the company as well as information security consultants. However, it was also observed that most of the risks’ values were slightly different or they were very close. This might have occurred due to the fact that in this study, asset values and risk probability values were not real continuous values but experts’ rankings between 1 and 10, which provided very similar resultant values. If real monetary values for the assets and real probability values could have been used, the risk values would not have been so close to each other. It should be noted that due to the conditional and marginal probabilities calculated by the Bayesian network model might have also affected this closeness issue.

CHAPTER FOUR
CONCLUSION

In this paper, a new information security risk assessment model is proposed which is based on Bayesian network model and Fuzzy inference system. The aim of combining these two methodologies is evaluating the qualitative and / or quantitative risks in a more reliable, flexible, and objective manner. This information security risk assessment approach is different from other methodologies in the literature by combining the Bayesian network model and fuzzy inference system.

This proposed model is constructed for a software services company in order to evaluate the information security risk factors based on their test procedures and test processes. First of all, the system's assets, threats, and vulnerabilities have been thoroughly analysed with the experts in the selected company. Also, two information security experts contributed to analyzing the system and based on their opinions two additional risk element were added. Then, all information risk factors, threats, vulnerabilities, and their relations have been modelled in a Bayesian network model. GeNIe program was used in order to complete this step. Data was collected for our risk assessment model with experts and managers, based on the testing process in the company. Assets, vulnerabilities, threats, and related risk values were identified and analysed. Bayesian network model is constructed for identified vulnerabilities, risks, and their relations. Afterwards, marginal probabilities for each risk factor are calculated. After Bayesian network model is constructed, fuzzy membership functions are designed for assets' values, risks' probabilities, and risk values. In order to obtain more reliable and less subjective approach to the risk assessment process, fuzzy inference system has been used in this new model. Fuzzy decision rules are constructed for some of the chosen risks by using the assets' values, relative risk values and relevant risk probabilities. Ultimately, the aggregation and defuzzification processes are completed by using the risk impact values. Based on the final risk values, the risks are evaluated according to the relevant assets, maximum risk values were obtained, and they were finally ranked for information security risk assessment process.

It should be mentioned that the proposed novel model can be flexibly and easily adapted to different companies' and organizations' information security risk assessment processes within their diverse information security management scopes. Anyone can adapt and use this model for their organization by either quantitative values / scores, or qualitative measures, or both.

REFERENCES

Altuzarra, A., Moreno-Jiménez, J. M. & Salvador, M. (2007). A Bayesian priorization procedure for AHP-group decision making. *European Journal of Operational Research, 182*(1), 367-382.

Ariyanti, R. D., Kusumadewi, S., & Paputungan, I. V. (2010). Beck depression inventory test assessment using fuzzy inference system. In 2010 *International Conference on Intelligent Systems, Modelling and Simulation* (6-9). IEEE.

Aslam, A., Ahmad, N., Saba, T., Almazyad, A. S., Rehman, A., Anjum, A. & Khan, A. (2017). Decision support system for risk assessment and management strategies in distributed software development. *IEEE Access*, *5*, 20349-20373.

Awad, G. A., Sultan, E. I., Ahmad, N., Ithnan, N., & Beg, A. H. (2011). Multi-objectives model to process security risk assessment based on AHP-PSO. *Modern Applied Science*, *5*(3), 246.

Barber, D. (2011). *Bayesian reasoning and machine learning*, UK: Cambridge University Press.

BayesFusion, LLC (n.d.), *GeNIe modeler: complete modeling freedom*, Retrieved March 6, 2019 from https://www.bayesfusion.com/genie/.

Bayraktarli, Y. Y., Ulfkjaer, J. P., Yazgan, U., & Faber, M. H. (2005). On the application of Bayesian probabilistic networks for earthquake risk management. In *9th International Conference on Structural Safety and Reliability (ICOSSAR 05)*, 20-23.

Beken S. & Eminağaoğlu M. (2018). Information security risk assessment using Bayesian network and fuzzy inference system: a case study, *ICATCES2018,*

Proceedings of International Conference on Advanced Technologies, Computer Engineering and Science, May 11-13, 2018, Safranbolu, Turkey, 1-8.

Bruner B. (n.d.). *Marginal & conditional probability distributions: definition & examples.* Retrieved March 25, 2019 from https://study.com/academy/lesson/marginal-conditional-probability-distributions-definition-examples.html.

Chin, K. S., Tang, D. W., Yang, J. B., Wong, S. Y., & Wang, H. (2009). Assessing new product development project risk by Bayesian network with a systematic probability generation methodology. *Expert Systems with Applications*, *36*(6), 9879-9890.

Committee on National Security Systems. (2010). *National Information Assurance (IA) Glossary*.

Denys, P. (2006). Efficiency of risk assessment methods, *Proceedings of IEEE Modern Problems of Radio Engineering, Telecommunications and Computer Science,* 353-354. IEEE.

Enterprise, S. (2005). *The logic behind CRAMM's assessment of measures of risk and determination of appropriate countermeasures,* Technical report. Retrieved July 07, 2018 from http://www.cramm.com/downloads/techpapers.htm.

Foroughi, F. (2008). Information security risk assessment by using Bayesian learning technique. *In Proceedings of the World Congress on Engineering*, *1*(27), 133-138.

Frigault, M., Wang, L., Singhal, A. & Jajodia, S. (2008). Measuring network security using dynamic bayesian network. *In Proceedings of the 4th ACM workshop on Quality of protection*, 23-30. ACM.

Fu, S. & Xiao, Y. (2012). Strengthening the research of information security risk assessment. *Advances in Biomedical Engineering*, *9*, 386-392.

Glen S. (2014), *Marginal distribution.* Retrieved March 25, 2019 from https://www.statisticshowto.datasciencecentral.com/marginal-distribution/.

ISO, (2011), ISO/IEC 27005. *Information security risk management.* Geneva: International Organization for Standardization.

ISO, (2013), ISO/IEC 27001. *Information security management systems, information technology, security techniques.* Geneva: international organization for standardization.

Karabacak, B. & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147-159.

Landoll, D. J., & Landoll, D. (2005). *The security risk assessment handbook: A complete guide for performing security risk assessments.* London: CRC Press.

Lee, M. C. (2014). Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *International Journal of Computer Science & Information Technology*, *6*(1), 29.

Li, S., Bi, F., Chen, W., Miao, X., Liu, J. & Tang, C. (2018). An improved information security risk assessments method for cyber-physical-social computing and networking. *IEEE Access*, *6*, 10311-10319.

Maglogiannis, I., Zafiropoulos, E., Platis, A., & Lambrinoudakis, C. (2006). Risk analysis of a patient monitoring system using Bayesian Network modeling. *Journal of Biomedical Informatics*, *39*(6), 637-647.

Marmer V. (2014). *Conditional probability, independence, bayes' rule*. Retrieved March 24, 2019 from http://faculty.arts.ubc.ca/vmarmer/econ327/327_02_cond_probability.pdf.

MathWorks, Inc., (n.d.), *Fuzzy logic toolbox.* Retrieved March 6, 2019 from https://www.mathworks.com/products/fuzzy-logic/features.html.

NIST National Institute of Standards and Technology. (2011). *Guide for conducting risk assessments*. Special Publication 800 - 30 rev.1, USA.

Ross, T. J. (2004). *Fuzzy logic with engineering applications*, 2nd edition. New York: John Wiley & Sons Ltd.

Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications, 18*(1), 45-52.

Takçı, H., Akyüz, T., Uğur, A., Karabağ, R., Aktaş, F. Ö., & Soğukpınar, İ. (2010). Bilgi güvenliği yönetiminde risk değerlendirmesi için bir model. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 3*(1), 47-52.

The Marginal Probability Functions. (n.d). Retrieved March 25, 2019, from https:// www.chegg.com/ homework - help/ definitions/ the - marginal- probability-functions-31.

Wang, J., Fan, K., Mo, W. & Xu, D. (2016). A method for information security risk assessment based on the dynamic Bayesian network. In *2016 International Conference on Networking and Network Applications (NaNA)*, 279-283. IEEE.

Wawrzyniak, D. (2006). Information security risk assessment model for risk management. In *International Conference on Trust, Privacy and Security in Digital Business* (21-30). Springer, Berlin, Heidelberg.

Wu, X., Fu, Y., & Wang, J. (2009). Information systems security risk assessment on improved fuzzy AHP. In *2009 ISECS international colloquium on computing, communication, control, and management*, *4*, 365-369. IEEE.

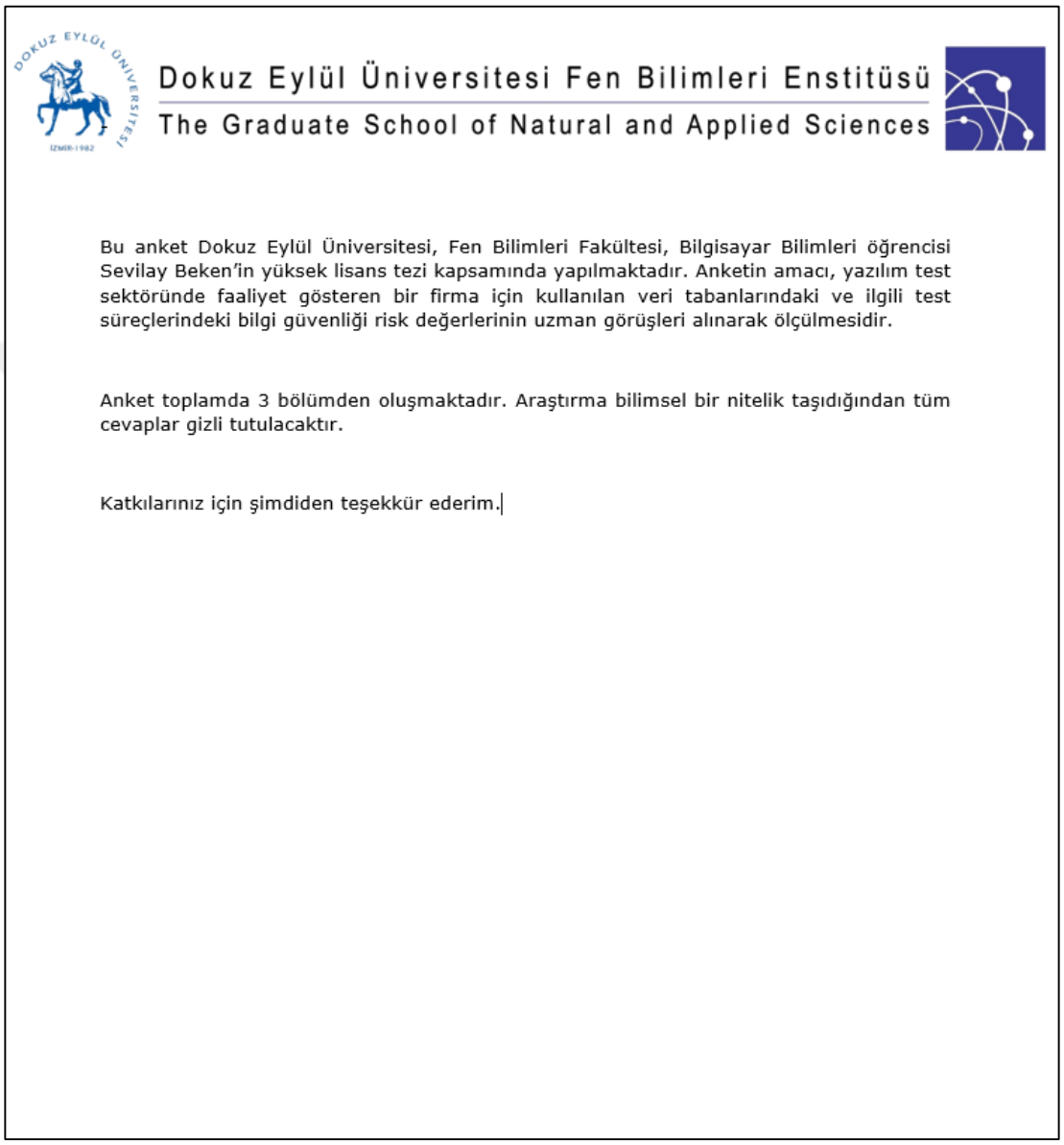
Yong, Q., Long, X., & Qianmu, L. (2008). Information security risk assessment method based on CORAS frame. In *2008 International Conference on Computer Science and Software Engineering*, *3*, 571-574. IEEE.

Yuhan, H., Xiaoyan, C., Linqiao, D., Songsong, Z., Min, W. & Yanxiong, H. (2013). The reclamation soil suitability study of the highway dumping site based on fuzzy comprehensive evaluation method. *Nature Environment and Pollution Technology*, *12*(1), 51.

Zhao, D. M., Wang, J. H., Wu, J. & Ma, J. F. (2005). Using fuzzy logic and entropy theory to risk assessment of the information security. In *2005 International Conference on Machine Learning and Cybernetics*, *4*, 2448-2453. IEEE.

APPENDICES

APPENDIX 1: Information Security Evaluation Form In Order to Get Experts' Opinions



Dokuz Eylül Üniversitesi Fen Bilimleri Enstitüsü
The Graduate School of Natural and Applied Sciences

Bu anket Dokuz Eylül Üniversitesi, Fen Bilimleri Fakültesi, Bilgisayar Bilimleri öğrencisi Sevilay Beken'in yüksek lisans tezi kapsamında yapılmaktadır. Anketin amacı, yazılım test sektöründe faaliyet gösteren bir firma için kullanılan veri tabanlarındaki ve ilgili test süreçlerindeki bilgi güvenliği risk değerlerinin uzman görüşleri alınarak ölçülmesidir.

Anket toplamda 3 bölümden oluşmaktadır. Araştırma bilimsel bir nitelik taşıdığından tüm cevaplar gizli tutulacaktır.

Katkılarınız için şimdiden teşekkür ederim.

APPENDIX 1: continues

1. BÖLÜM

*Aşağıdaki durumların belirtilen ölçeklendirme derecelerine göre **tehdit** düzeylerini belirleyiniz.*

(1: Düşük, 2: Orta, 3:Yüksek)

	1	2	3
Teknik sorunlar nedeniyle bilgisayarınızın çalışmama olasılığı nedir?			
Virüs vb. zararlı yazılımlar nedeniyle bilgisayarınıza erişim sorunu yaşama olasılığı nedir?			
Elektrik kesintilerinin bilgisayar kullanımınız üzerinde yaratacağı olumsuz etki düzeyi nedir?			
Virüs vb. zararlı yazılımların veri tabanı sistemine zarar verme olasılığı nedir?			
Virüs vb. zararlı yazılımların VPN üzerinden bilgisayarınıza bulaşma olasılığı nedir?			
Teknik sorunlar nedeniyle VPN erişiminde sorun yaşanma olasılığı nedir?			
Elektrik kesintilerinin ofis ortamında çalışmanız üzerinde yaratacağı olumsuz etki düzeyi nedir?			
Yangın vb. sorunların iş sürecinize olumsuz etki düzeyi nedir?			
Deprem vb. doğal afetler yaşanmasının iş sürecinize olumsuz etki düzeyi nedir?			
Bilgisayarınızın çalınması/kaybolması durumunda önemli bilgilerin kaybolma olasılığı nedir?			
IT uzmanlarının yeterli teknik eğitim almamasının olumsuz etki düzeyi nedir?			
IT uzmanlarının bilgi güvenliği konusundaki bilgisizliği veya dikkatsizliği iş süreçlerini ne ölçüde etkiler?			
Veri tabanındaki müşteri bilgilerinin IT uzmanlarınca yetki veya kural dışı kullanılma olasılığı nedir?			
Bilişim suçlularının müşteri bilgilerine erişerek bilgileri çalma olasılığı nedir?			
VPN üzerinden bilişim suçlularının veri tabanına erişebilme olasılığı nedir?			
Veri tabanındaki müşteri bilgilerinin Test uzmanlarınca yetki veya kural dışı kullanılma olasılığı nedir?			
Test uzmanlarının yeterli eğitim almamasının olumsuz etki düzeyi nedir?			
Test uzmanlarının bilgi güvenliği konusundaki bilgisizliği veya dikkatsizliği iş süreçlerini ne ölçüde etkiler?			
Veri tabanındaki müşteri bilgilerinin Test Destek uzmanlarınca yetki veya kural dışı kullanılma olasılığı nedir?			
Test Destek uzmanlarının yeterli teknik eğitim almamasının olumsuz etki düzeyi nedir?			
Test Destek uzmanlarının bilgi güvenliği konusundaki bilgisizliği veya dikkatsizliği iş süreçlerini ne ölçüde etkiler?			

APPENDIX 1: continues

2. BÖLÜM

*Aşağıdaki senaryolar için belirtilen ölçeklendirme derecelerine göre **risk** düzeylerini belirleyiniz.*

(1:Çok Düşük Risk,2:Düşük Risk,3:Orta Dereceli Risk,4:Yüksek Risk,5:Çok Yüksek Risk)

	1	2	3	4	5
Bilgisayarınızda oluşan teknik sorunlar nedeniyle bilgisayarınızın kullanılamaması					
Virüs vb. zararlı yazılımlar nedeniyle bilgisayarınızın kullanılamaması					
Elektrik kesintileri nedeniyle bilgisayarınızın kullanılamaması					
Yangın vb. sorunlar nedeniyle bilgisayarınızın kullanılamaması					
Deprem vb. doğal afetler yaşanması nedeniyle bilgisayarınızın kullanılamaması					
Bilgisayarınızda çalınması veya kaybolması nedeniyle bilgisayarın kullanılamaması					
Bilgisayarınızda oluşan teknik sorunlar nedeniyle veri tabanına erişiminizin kesilmesi					
Virüs vb. zararlı yazılımlar nedeniyle veri tabanına erişiminizin kesilmesi					
Test uzmanlarının hatası nedeniyle veri tabanına erişiminizin kesilmesi					
IT uzmanlarının hatası nedeniyle veri tabanına erişiminizin kesilmesi					
Test destek uzmanlarının hatası nedeniyle veri tabanına erişiminizin kesilmesi					
Bilişim suçlularının müdahalesi nedeniyle veri tabanına erişiminizin kesilmesi					
Virüs vb. zararlı yazılımlar nedeniyle veri tabanındaki verilerin silinmesi veya kaybolması					
Test uzmanlarının hatalı uygulamaları nedeniyle veri tabanındaki bilgilerin silinmesi/ kaybolması					
Bilişim suçlularının müdahalesi nedeniyle veri tabanındaki bilgilerin silinmesi/ kaybolması					
Virüs vb. zararlı yazılımlar nedeniyle veri tabanına erişilememesi					
Test destek ekiplerinin hatalı uygulamaları nedeniyle veri tabanına erişilememesi					
Bilişim suçlularının müdahalesi nedeniyle veri tabanına erişilememesi					
Bilgisayarınızın çalınması/kaybolması durumunda hassas müşteri bilgilerinin kaybedilmesi					
Test uzmanlarının hatası nedeniyle hassas müşteri bilgilerinin kaybedilmesi					
IT uzmanlarının hatası nedeniyle hassas müşteri bilgilerinin kaybedilmesi					

APPENDIX 1: continues

Test Destek uzmanlarının hatası nedeniyle hassas müşteri bilgilerinin kaybedilmesi					
Bilişim suçlularının müdahalesi ilehassas müşteri bilgilerininkaybedilmesi					
Veri tabanındaki bilgilerin yetki veya kural dışı kullanılması nedeniyle hassas müşteri bilgilerinin kaybedilmesi					
Kullanıcıların bilgisizliği/deneyimsizliği nedeniyle verilerin bozulması					
Bilişim suçlularının müdahalesi nedeniyle verilerin bozulması					
Bilgisayarınızı kullanamıyor olmanız nedeniyle test süreçlerinde aksaklık yaşanması					
Veri tabanlarına erişim sağlanamaması nedeniyle test süreçlerinde aksaklık yaşanması					
Veri tabanındaki veri kayıpları nedeniyle test süreçlerinde aksaklık yaşanması					
Veri tabanı sistemine erişilememesi nedeniyle test süreçlerinde aksaklık yaşanması					
Verilerin değiştirilmesine bağlı olarak test süreçlerinde hatalı sonuçlar alınması					
Test süreçlerinde aksama yaşanması durumunda firmanızın yaşayacağı itibar kaybı					
Müşteri bilgilerinin çalınması / art niyetli olarak ele geçirilmesi durumunda firmanızın yaşayacağı itibar kaybı					
Hatalı test sonuçları alınması durumunda firmanızın yaşayacağı itibar kaybı					

3. BÖLÜM

Aşağıdaki bilgi varlıklarının yaklaşık değerlerini 1'den 10'a kadar belirtilen ölçüde ***veya*** *yaklaşık değerini (TL cinsinden) değerlendiriniz.*

(1:Çok Düşük-10:Çok Yüksek)

	1 .. 10	Yaklaşık Değer (TL)
Bilgisayarlarınızdaki veriler		
IT Uzmanlarının Bilgi ve Deneyimi		
Veri tabanındaki Müşteri Bilgileri		
Test Verileri		
VPN Bağlantısı		
Test Uzmanlarının Bilgi ve Deneyimi		
Test Destek Uzmanlarının Bilgi ve Deneyimi		

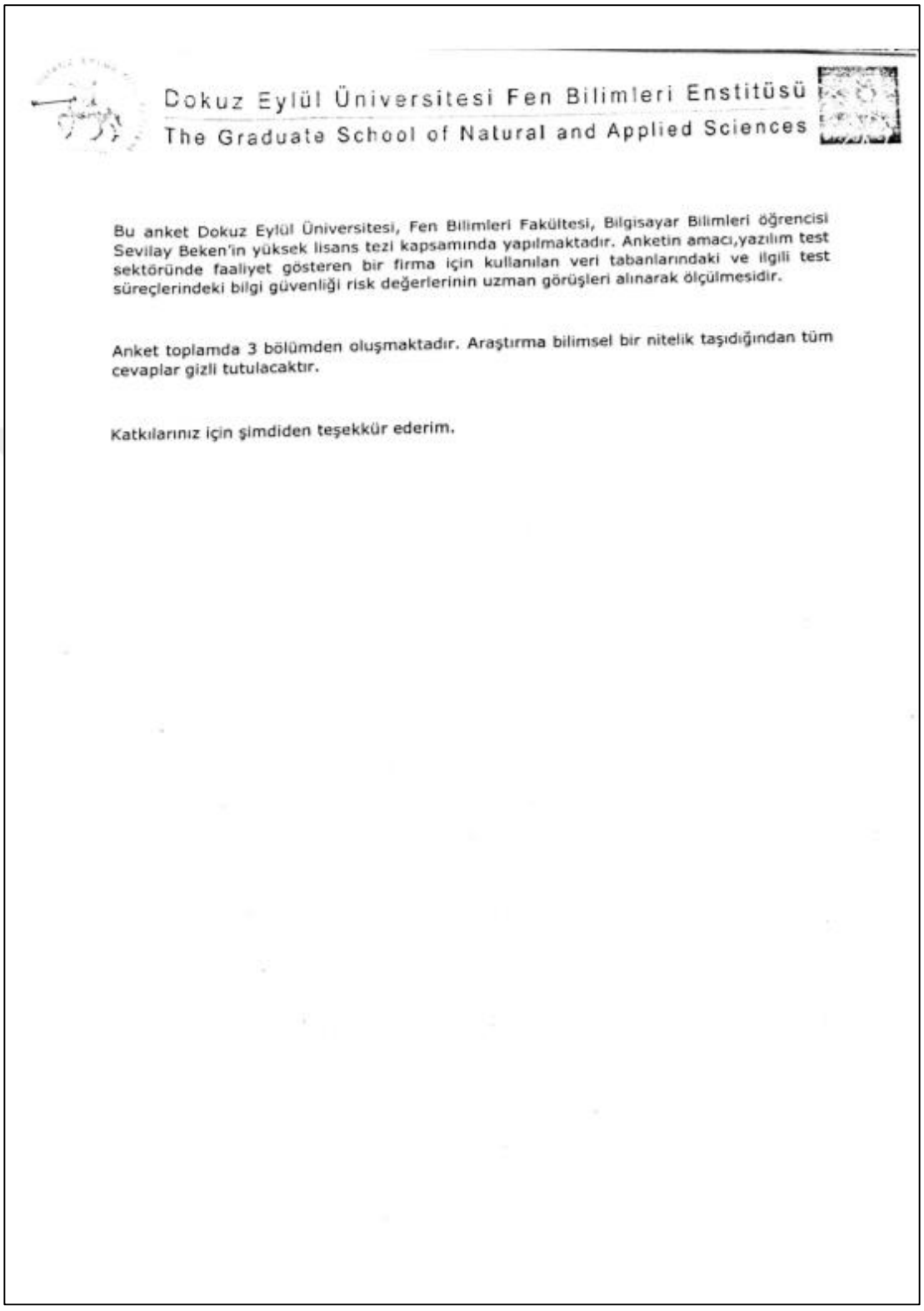
APPENDIX 1: continues

*Aşağıdaki senaryolar için belirtilen ölçeklendirme derecelerine göre **risk** düzeylerini belirleyiniz.*

(1:Çok Düşük Risk,2:Düşük Risk,3:Orta Dereceli Risk,4:Yüksek Risk,5:Çok Yüksek Risk)

	1	2	3	4	5
Test süreçlerinde aksaklık yaşanması sebebiyle iş gücü kaybı yaşanması					
Müşteri bilgilerinin çalınması / art niyetli olarak ele geçirilmesi durumunda firmanıza uygulanacak yasal yaptırımlar ve cezai işlemler					

APPENDIX 2: An Example Evaluation Form Which Was Filled By An Expert



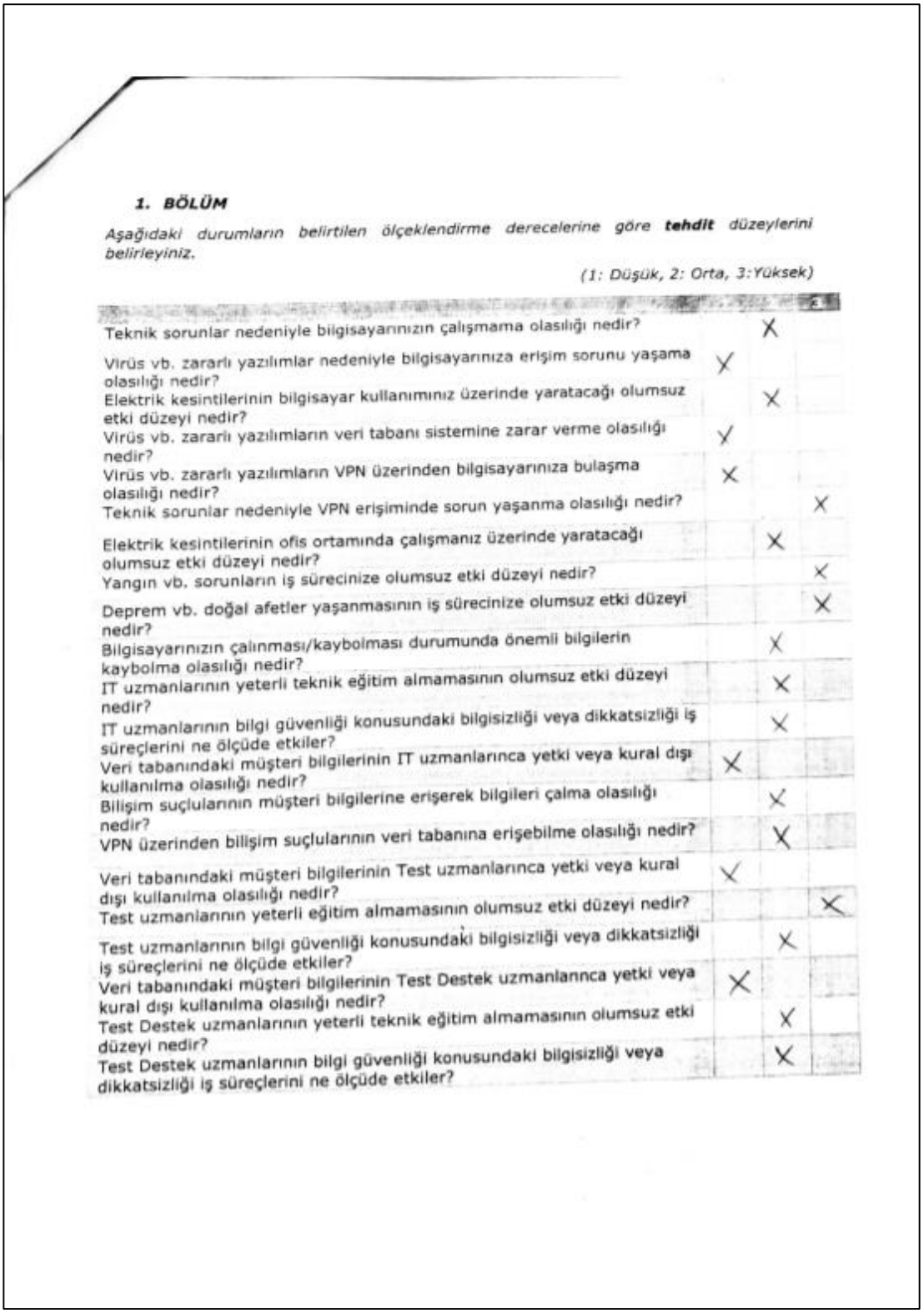
Dokuz Eylül Üniversitesi Fen Bilimleri Enstitüsü
The Graduate School of Natural and Applied Sciences

Bu anket Dokuz Eylül Üniversitesi, Fen Bilimleri Fakültesi, Bilgisayar Bilimleri öğrencisi Sevilay Beken'in yüksek lisans tezi kapsamında yapılmaktadır. Anketin amacı,yazılım test sektöründe faaliyet gösteren bir firma için kullanılan veri tabanlarındaki ve ilgili test süreçlerindeki bilgi güvenliği risk değerlerinin uzman görüşleri alınarak ölçülmesidir.

Anket toplamda 3 bölümden oluşmaktadır. Araştırma bilimsel bir nitelik taşıdığından tüm cevaplar gizli tutulacaktır.

Katkılarınız için şimdiden teşekkür ederim.

APPENDIX 2: continues



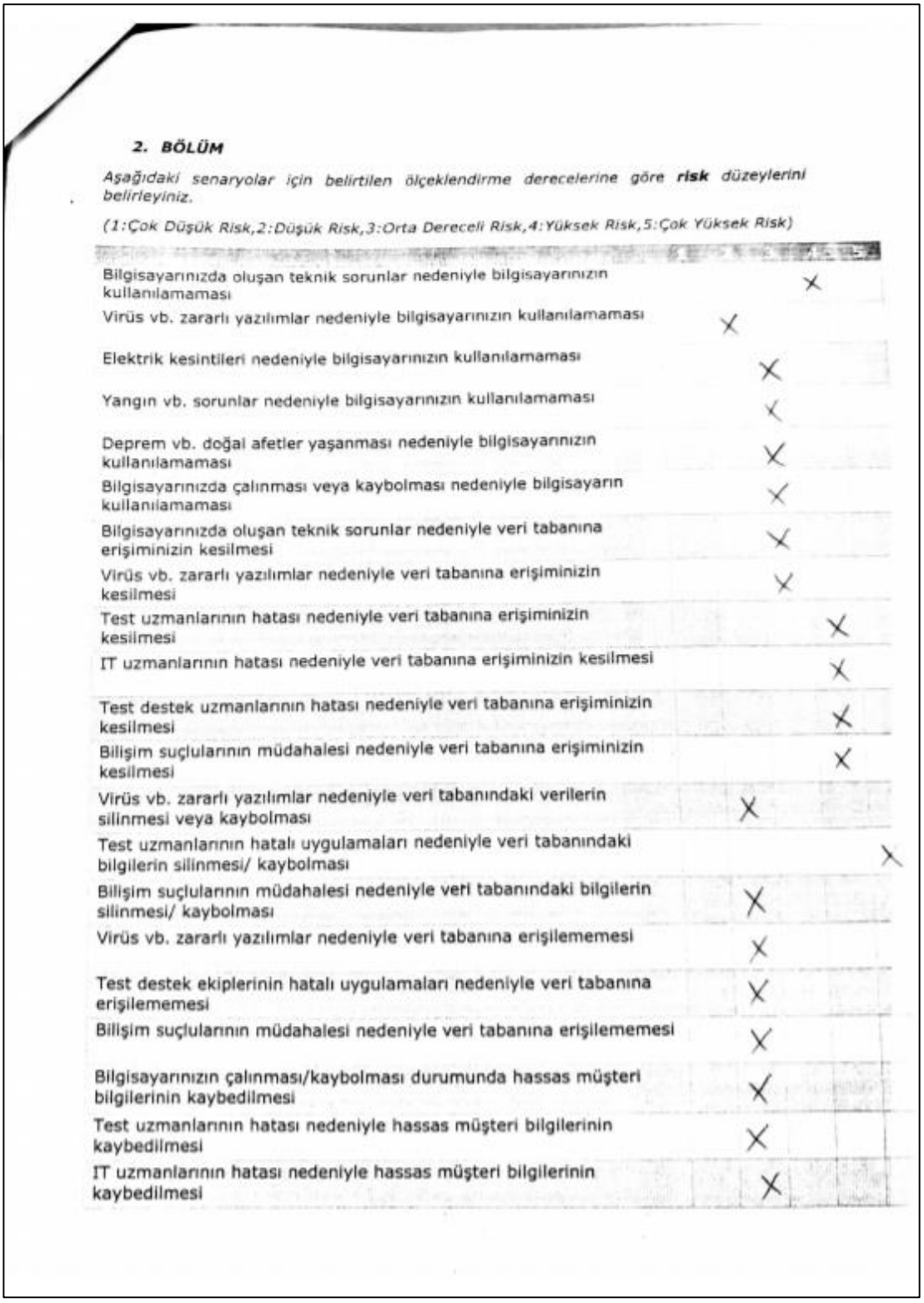
1. BÖLÜM

Aşağıdaki durumların belirtilen ölçeklendirme derecelerine göre ***tehdit*** *düzeylerini belirleyiniz.*

(1: Düşük, 2: Orta, 3:Yüksek)

Teknik sorunlar nedeniyle bilgisayarınızın çalışmama olasılığı nedir?		X	
Virüs vb. zararlı yazılımlar nedeniyle bilgisayarınıza erişim sorunu yaşama olasılığı nedir?	X		
Elektrik kesintilerinin bilgisayar kullanımınız üzerinde yaratacağı olumsuz etki düzeyi nedir?		X	
Virüs vb. zararlı yazılımların veri tabanı sistemine zarar verme olasılığı nedir?	X		
Virüs vb. zararlı yazılımların VPN üzerinden bilgisayarınıza bulaşma olasılığı nedir?	X		
Teknik sorunlar nedeniyle VPN erişiminde sorun yaşanma olasılığı nedir?			X
Elektrik kesintilerinin ofis ortamında çalışmanız üzerinde yaratacağı olumsuz etki düzeyi nedir?		X	
Yangın vb. sorunların iş sürecinize olumsuz etki düzeyi nedir?			X
Deprem vb. doğal afetler yaşanmasının iş sürecinize olumsuz etki düzeyi nedir?			X
Bilgisayarınızın çalınması/kaybolması durumunda önemli bilgilerin kaybolma olasılığı nedir?		X	
IT uzmanlarının yeterli teknik eğitim almamasının olumsuz etki düzeyi nedir?		X	
IT uzmanlarının bilgi güvenliği konusundaki bilgisizliği veya dikkatsizliği iş süreçlerini ne ölçüde etkiler?		X	
Veri tabanındaki müşteri bilgilerinin IT uzmanlarınca yetki veya kural dışı kullanılma olasılığı nedir?	X		
Bilişim suçlularının müşteri bilgilerine erişerek bilgileri çalma olasılığı nedir?		X	
VPN üzerinden bilişim suçlularının veri tabanına erişebilme olasılığı nedir?		X	
Veri tabanındaki müşteri bilgilerinin Test uzmanlarınca yetki veya kural dışı kullanılma olasılığı nedir?	X		
Test uzmanlarının yeterli eğitim almamasının olumsuz etki düzeyi nedir?			X
Test uzmanlarının bilgi güvenliği konusundaki bilgisizliği veya dikkatsizliği iş süreçlerini ne ölçüde etkiler?		X	
Veri tabanındaki müşteri bilgilerinin Test Destek uzmanlarınca yetki veya kural dışı kullanılma olasılığı nedir?	X		
Test Destek uzmanlarının yeterli teknik eğitim almamasının olumsuz etki düzeyi nedir?		X	
Test Destek uzmanlarının bilgi güvenliği konusundaki bilgisizliği veya dikkatsizliği iş süreçlerini ne ölçüde etkiler?		X	

APPENDIX 2: continues



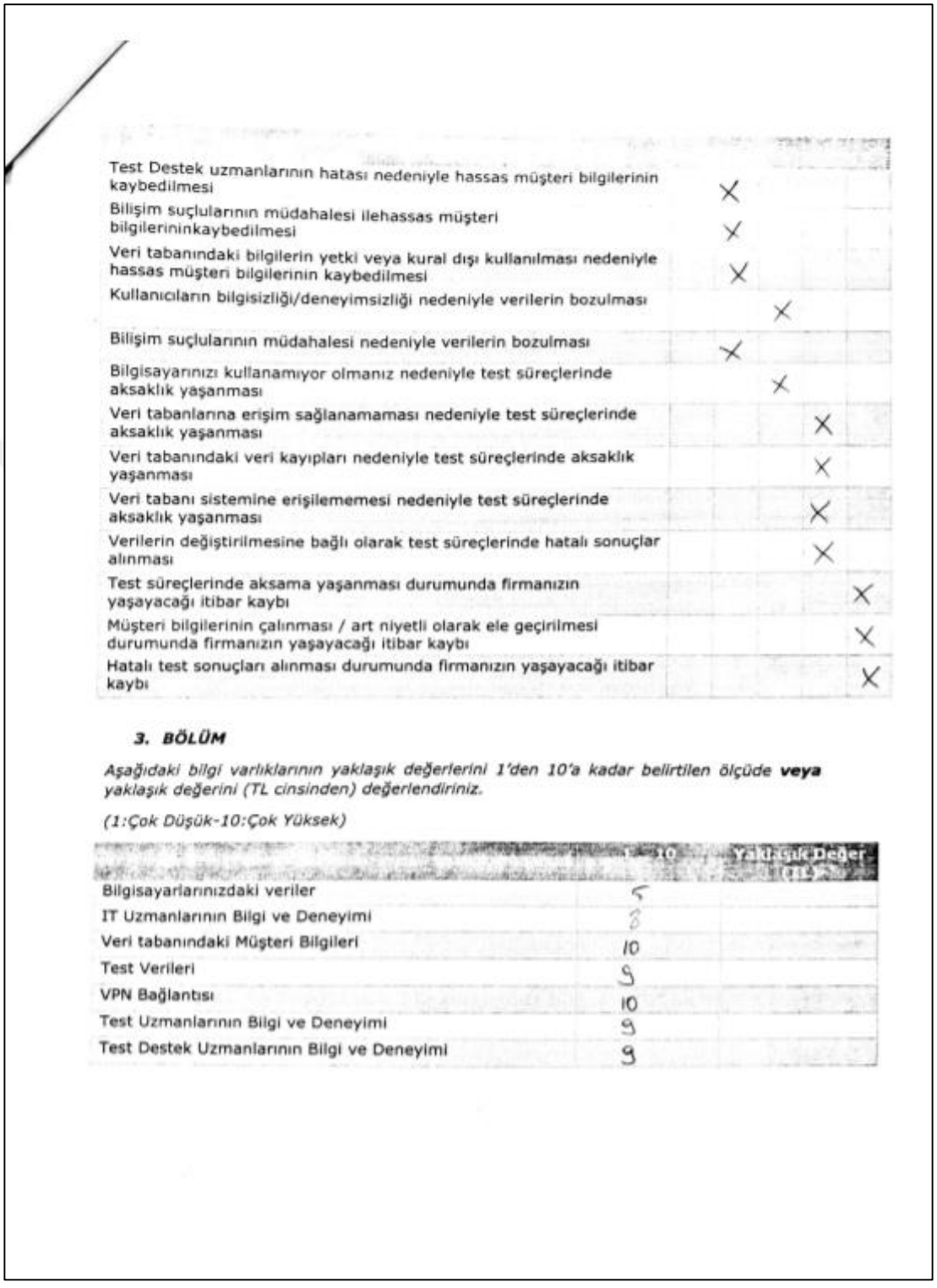
2. BÖLÜM

Aşağıdaki senaryolar için belirtilen ölçeklendirme derecelerine göre ***risk*** *düzeylerini belirleyiniz.*

(1:Çok Düşük Risk,2:Düşük Risk,3:Orta Dereceli Risk,4:Yüksek Risk,5:Çok Yüksek Risk)

Bilgisayarınızda oluşan teknik sorunlar nedeniyle bilgisayarınızın kullanılamaması				X	
Virüs vb. zararlı yazılımlar nedeniyle bilgisayarınızın kullanılamaması		X			
Elektrik kesintileri nedeniyle bilgisayarınızın kullanılamaması			X		
Yangın vb. sorunlar nedeniyle bilgisayarınızın kullanılamaması			X		
Deprem vb. doğal afetler yaşanması nedeniyle bilgisayarınızın kullanılamaması			X		
Bilgisayarınızda çalınması veya kaybolması nedeniyle bilgisayarın kullanılamaması			X		
Bilgisayarınızda oluşan teknik sorunlar nedeniyle veri tabanına erişiminizin kesilmesi			X		
Virüs vb. zararlı yazılımlar nedeniyle veri tabanına erişiminizin kesilmesi			X		
Test uzmanlarının hatası nedeniyle veri tabanına erişiminizin kesilmesi					X
IT uzmanlarının hatası nedeniyle veri tabanına erişiminizin kesilmesi					X
Test destek uzmanlarının hatası nedeniyle veri tabanına erişiminizin kesilmesi					X
Bilişim suçlularının müdahalesi nedeniyle veri tabanına erişiminizin kesilmesi					X
Virüs vb. zararlı yazılımlar nedeniyle veri tabanındaki verilerin silinmesi veya kaybolması			X		
Test uzmanlarının hatalı uygulamaları nedeniyle veri tabanındaki bilgilerin silinmesi/ kaybolması					X
Bilişim suçlularının müdahalesi nedeniyle veri tabanındaki bilgilerin silinmesi/ kaybolması			X		
Virüs vb. zararlı yazılımlar nedeniyle veri tabanına erişilememesi			X		
Test destek ekiplerinin hatalı uygulamaları nedeniyle veri tabanına erişilememesi			X		
Bilişim suçlularının müdahalesi nedeniyle veri tabanına erişilememesi			X		
Bilgisayarınızın çalınması/kaybolması durumunda hassas müşteri bilgilerinin kaybedilmesi			X		
Test uzmanlarının hatası nedeniyle hassas müşteri bilgilerinin kaybedilmesi			X		
IT uzmanlarının hatası nedeniyle hassas müşteri bilgilerinin kaybedilmesi			X		

APPENDIX 2: continues



Test Destek uzmanlarının hatası nedeniyle hassas müşteri bilgilerinin kaybedilmesi	X			
Bilişim suçlularının müdahalesi ilehassas müşteri bilgilerininkaybedilmesi	X			
Veri tabanındaki bilgilerin yetki veya kural dışı kullanılması nedeniyle hassas müşteri bilgilerinin kaybedilmesi	X			
Kullanıcıların bilgisizliği/deneyimsizliği nedeniyle verilerin bozulması		X		
Bilişim suçlularının müdahalesi nedeniyle verilerin bozulması	X			
Bilgisayarınızı kullanamıyor olmanız nedeniyle test süreçlerinde aksaklık yaşanması		X		
Veri tabanlarına erişim sağlanamaması nedeniyle test süreçlerinde aksaklık yaşanması			X	
Veri tabanındaki veri kayıpları nedeniyle test süreçlerinde aksaklık yaşanması			X	
Veri tabanı sistemine erişilememesi nedeniyle test süreçlerinde aksaklık yaşanması			X	
Verilerin değiştirilmesine bağlı olarak test süreçlerinde hatalı sonuçlar alınması			X	
Test süreçlerinde aksama yaşanması durumunda firmanızın yaşayacağı itibar kaybı				X
Müşteri bilgilerinin çalınması / art niyetli olarak ele geçirilmesi durumunda firmanızın yaşayacağı itibar kaybı				X
Hatalı test sonuçları alınması durumunda firmanızın yaşayacağı itibar kaybı				X

3. BÖLÜM

Aşağıdaki bilgi varlıklarının yaklaşık değerlerini 1'den 10'a kadar belirtilen ölçüde ***veya*** *yaklaşık değerini (TL cinsinden) değerlendiriniz.*

(1:Çok Düşük-10:Çok Yüksek)

	1-10	Yıllık Değer (TL)
Bilgisayarlarınızdaki veriler	5	
IT Uzmanlarının Bilgi ve Deneyimi	3	
Veri tabanındaki Müşteri Bilgileri	10	
Test Verileri	9	
VPN Bağlantısı	10	
Test Uzmanlarının Bilgi ve Deneyimi	9	
Test Destek Uzmanlarının Bilgi ve Deneyimi	9	