SUPPLEMENTING ISRM MODELS BY KRI IMPLEMENTATION

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF SOCIAL SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

FUAT ÖZÇAKMAK

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF SCIENCE AND TECHNOLOGY POLICY STUDIES

JULY 2019

Approval of the Graduate School of Social Sciences

Prof. Dr. Tülin Gençöz
Director

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

Prof. Dr. Teoman Pamukçu
Head of Department

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

Dr. Ali Arifoğlu
Co-Supervisor

Assist. Prof. Dr. Aybar Can Acar
Supervisor

Examining Committee Members

Assoc. Prof. Dr. Aysu Betin Can (METU, IS) _____

Assist. Prof. Dr. Aybar Can Acar (METU, HI) _____

Prof. Dr. Serpil Aktaş Altunay (Hacettepe Uni., İST) _____

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

Name, Last name : Fuat ÖZÇAKMAK

Signature :

ABSTRACT

SUPPLEMENTING ISRM MODELS BY KRI IMPLEMENTATION

ÖZÇAKMAK, Fuat
M.Sc., Department of Science and Technology Policy Studies
Supervisor: Asst. Prof. Aybar Can ACAR
Co-Supervisor: Dr. Ali ARİFOĞLU

July 2019, 122 pages

Cybersecurity efforts should be spent effectively and timely with regard to where and when they are needed because of the resource requirements. In order to secure Information Technology (IT) systems, The Information Systems Risk Management (ISRM) standards like ISO 27000, NIST 800 series and COBIT 5 frameworks are used as best practices. These standards use a diversity of metrics to monitor the Information Security Management System (ISMS). However, large amounts of money, time and human resources are needed to detect, measure and interpret all. Moreover, these standards do not deal with the resources allocated and senior managements' concern. To avoid these concerns, Key Risk Indicator (KRI) based risk monitoring can help a significant decrease in the required resources and increase the risk monitoring effectiveness. In this study, a new KRI implementation model that can facilitate risk management, figure out costs, benefits and address stakeholders' concerns, for ISRM standards is proposed.

Keywords: Information Security Risk Management, Cybersecurity Risk Assessment, Key Risk Indicators, Cybersecurity Metrics, Cost of Cybersecurity.

ÖZ

ARG UYGULAYARAK BSRY MODELLERİNİN GELİŞTİRİLMESİ

ÖZÇAKMAK, Fuat
Yüksek Lisans, Bilim ve Teknoloji Politikası Çalışmaları Bölümü
Tez Danışmanı: Dr. Öğr. Üyesi Aybar Can ACAR
Yardımcı Tez Danışmanı: Dr. Ali ARİFOĞLU

Temmuz 2019, 122 sayfa

Siber güvenlik gayretleri ihtiyaç duyuldukları zaman ve yere bağlı olarak etkili ve zamanlı kullanılmalıdır çünkü bu gayretler için kaynak gerekmektedir. Bilgi Sistemlerini (BS) korumak için, ISO 27000, NIST 800 serisi ve COBIT 5 çerçeveleri gibi Bilgi Sistemleri Risk Yönetimi (BSRY) standartları en iyi uygulamalar olarak kullanılmaktadır. Bu standartlar, Bilgi Güvenliği Yönetim Sistemini (BGYS) izlemek için çeşitli ölçümleri kullanmaktadır. Bununla birlikte, hepsini tespit etmek, ölçmek ve yorumlamak için çok büyük para, zaman ve personel gerekmektedir. Ayrıca bu standartlar, kaynaklar ve yönetiminin endişeleri ile ilgilenmemektedir. Bu endişeleri gidermek için, Anahtar Risk Göstergesi (ARG) temelli risk izleme, kaynaklarda önemli bir tasarrufa ve risk izleme etkinliğini arttırmaya yardımcı olabilir. Bu çalışmada, BSRY standartları için risk yönetimini kolaylaştırabilen, paydaşların endişelerini gözeten yeni bir ARG uygulama modeli önerilmiştir.

Anahtar Kelimeler: Bilgi Güvenliği Risk Yönetimi, Siber Güvenlik Risk Değerlendirme, Anahtar Risk Göstergeleri, Siber Güvenlik Metrikleri, Siber Güvenlik Maliyeti.

To METU, and my Family

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Asst.Prof. Aybar Can ACAR and co-supervisor: Dr.Ali ARİFOĞLU for their extensive support, guidance and patience throughout my thesis studies. I am grateful for what they have done for me so far.

Special thanks to the Company and its CISO and engineers I worked with during case studies. It was fantastic to have the opportunity to work my research in your facilities.

I am also grateful to Dr.Hasan Çifci, Asst.Prof. Emin Kuğu, Prof.Dr.Serpil Aktaş Altunay, Meltem Eraykutlar, Mustafa Yılmaz, Bahtiyar Bircan, Murat Savcı and all participants of the survey for their unfailing support and assistance.

Last but not the least, I would like to thank my beloved wife Gülay Özçakmak and my sweet kids Bengisu and Asel Cansu for their boundless love, patience and supporting me spiritually throughout the thesis period.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CEO	Chief Executive Officer
CIA	Triad Confidentiality, Integrity, and Availability
CISO	Chief Information Security Officer
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technology.
CRO	Chief Risk Officer
DCSs	Distributed Control Systems
GDP	GROSS DOMESTIC PRODUCT
GISS	Global Information Security Survey
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISRM	Information Systems Risk Management
KRI	Key Risk Indicator
NIST	The National Institute of Standards and Technology
ROI	Return on Investment
ROSI	Return on Security Investment
SCADA	Supervisory Control and Data Acquisition

CHAPTER 1

INTRODUCTION

1.1. The Problem

> I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image. - Stephen Hawking

The cyber attacks can have us live our own Day of Resurrection personally, as well as the effects we can be socially affected. These attacks may be in a range that affects the financial market, health records, transport networks, energy, and military defense systems. Ensuring that the information is delivered to the decision makers in a precise, complete and timely manner increases the productivity of the enterprises.

Studies show that it is impossible to create a defensive structure for all of these threats because creating a defense against all threats would prevent our own system from functioning. Besides such a defense would require much more resource than the damage would give or the initial costs of our system. In addition, since the threats will never end, it will be necessary to take continuous action and this will be an infinite loop. Andrew Jaquith called this the alternative view of risk management as "The Hamster Wheel of Pain" and noted that similar schemes in risk management always cover the following four phases:

- Assessment (or detection),
- Reporting,
- Prioritization,
- Mitigation [1].

Besides making profound inquiry of the risk management models in which these four phases are involved, people often try to apply instantaneous known threats without quantitative value analysis and with resource limits ignored [1].

It is certain that the most efficient way to use cybersecurity resources is through risk management. However, because integrated cybersecurity management with risk management will attempt to take precautions against all detected risks, it will not be true to tell that resources are used effectively. In this case, the importance of monitoring the risks increases. On the other hand, since dozens of risks occur every day, monitoring all risks will be either impossible or very resource-intensive.

It is not known that many organizations failed because of cybersecurity events. The core reason for this uncertainty is the effective risk policies for disclosing and replying to hazards, and luck. Generally, not all failures in IT systems are associated with cybersecurity, but it is known that the operational effectiveness of many services is affected by cyber events. While the effectiveness, speed of development and complexity of cyber attacks increase, organizations that benefit from IT systems must adapt to the same pace and renew their risk strategies.[2].

Cybersecurity measures are taken appropriately with the risk management standards used today require a significant amount of cost. These costs also include the costs incurred for unrealized risks. In this case, resources are spent on risks that will never occur. The problem identified here is that ISRM standards obligate CISOs or Cybersecurity personnel to take measures against all risks. When these ISRM standards are implemented, resources are spent to eliminate all risks, and if new risks are identified and monitored then risk mitigation measures are taken again with additional resources. Nonetheless, the risks are unlimited, but resources are not. The risk monitoring chapters of ISRM standards need to be supplemented to reduce cybersecurity costs. In this way, limited resources will be used more effectively and unnecessary resources will not be wasted for the unrealized risks.

1.2. Motivation

Cybercrime is a sneaky threat reaching crisis levels. McAfee Global Cost of Cybercrime 2014 report asserts that global economic cost estimates for cybercrime can range from $375 billion to $575 billion per year although it is difficult to measure accurately [3]. As it is growing there is no system in the safe area. It is spreading and being stronger every day and its vaccine has not been found yet. Nicole Radziwill thinks that it takes time, effort, and money to protect the confidentiality, integrity, and accessibility of information. According to her research, firms usually concentrate on two points: making financial plan accordingly, and figuring out the fiscal significance of cyber attacks [4].

Companies, organizations, and nations are allocating a significant amount of budget for providing cybersecurity. All organizations investing in this issue allocate resources in accordance with the value of their IT systems and all related cyber assets. Bojanc and Blazic define the purpose of security controls applied in IT systems as to equalize the resources allocated for the mitigation of risk identified to the level of resources to be saved by reducing the risk [5].

The growth rate of spending on cybersecurity reflects not only the increasing use of IT systems but also the increased awareness of the threat. However, in researches, there is no information found showing the comparison of the expenditures made to ensure cybersecurity actually worked. On the other hand, the percentage of probability of occurrence in real-world risk is not significant when the risk is realized and the loss is met although the measures are taken according to the risk importance level.

Maybe senior management cannot believe in such a big thing would happen. In March 2011 risk world recorded the accident of the Fukushima nuclear plant because of an earthquake and tsunami. Again, it is wrong to say “However, we have taken steps to see that it will never happen again.” This is not a genuine description because of two reasons: “First, prudent managers will anticipate

potential disasters. Second, saying never implies that perfect security is the goal. This is nonsensical, since perfect security is infinitely expensive, and so cannot be achieved" [6].

Institutions need unlimited resources for cybersecurity because every day new threats and risks arise. While a lot of resources may be necessary to mitigate all these threats and risks, it may not always be possible to implement these measures as it is planned. Therefore, in any of the realistic risk management programs, the objective should not be zero risks. Risks should be measured by means of money just like resources. Therefore, the measures to be taken must be decided upon by a good evaluation.

Due to above issues, the aim of this study is to present a model to make risk monitoring function more effective by using KRIs and to enhance risk management activities of the international standards which considered as best practices to achieve safe IT Risk Management. By means of this model, risks that are about to be realized are detected and the resources allocated under the risk mitigation will be spent on time and avoid unnecessary resource allocation for the risks that will not be realized. In addition, risk management and monitoring procedures will be communicated more clearly with senior management. Top management's confidence in the technical team will also increase due to the use of resources only mitigating actual risks.

1.3. The Context of the Study

In this study, the improvement of the risk monitoring process with KRI in ISRM standards and its applications are investigated.

In the scope of the study, literature research was made using the keywords;

- Cybersecurity Key Risk Indicators,
- Cybersecurity Risk Assessment,
- ISO 27005,

- NIST 800,
- Information Security Risk Management System, and
- Information Security Management Systems Risk Assessment.

In addition;

- ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary (2016),
- ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements (2013),
- ISO/IEC 27004 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (2016 ed2),
- ISO/IEC 27005 Information technology — Security techniques — Information security risk management (2011 ed2),
- NIST 800-30 Guide for Conducting Risk Assessments (2012 Rev1),
- NIST 800-39 Managing Information Security Risk (2011),
- NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems (2011 rev1),
- NIST 800-55 Performance Measurement Guide for Information Security (2008 rev1), and
- NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (2011) standards were researched and after all researches using KRI in the ISRM could not be found.

On the other hand, when COBIT 5 for Risk was examined, it was found that, although KRI subject was mentioned the framework was based on scenario-based risk prevention methodology. Since COBIT 5 for Risk provide a top-level framework for arrangement of risk management activities it stands in the extent of ISO 31000:2009 – Risk Management, ISO 27005:2011 – Information Security Risk Management and COSO Enterprise Risk Management standards. When the framework was examined, issues related to risk management had been dealt within

the "EDM03 Ensure Risk Optimization" and "APO12 Manage Risk" processes and had not been covered in the extent of the study due to the content of the investigated standards.

Fourv Systems' report supports that the model proposed improving the risk management and monitoring in the context of using KRI can be implemented ISO/IEC 27000 and NIST 800 series standards or other ISRM standards and frameworks [7].

1.4. Sections of the Thesis

The context of the study was divided into chapters. In the first Chapter, the problem and the motivation of the study were explained.

In the second Chapter, the need for cybersecurity, projections of cyber threats, effective use of cybersecurity resources, the standards used for risk management were criticized.

In Chapter 3, the cost of cybersecurity was investigated and mitigating the cost of risks which never happened was researched.

In Chapter 4, the context of a systematic approach to ISRM and the need for it was questioned.

In Chapter 5, the definition, properties, developing, of KRI were summarized.

In Chapter 6, current ISRM standards and frameworks were reviewed.

In Chapter 7, the proposed model for Implementation of KRI into ISRM Processes was explained.

The current risk management models with the proposed model were compared in Chapter 8.

In Chapter 9, the result of the survey which was conducted to justify the Hypothesis of the thesis was assessed. The second step of the justification was done by a case study.

With the case study, proposed model was implemented into a company's ISMS and the implantation cycle detailed in the Chapter10.

At the end the study was summarized, concluded and future works were stated in Chapter 11.

CHAPTER 2

BACKGROUND

As the industrial world is replaced by information era, the structural change has made computer networks used in information infrastructure of all transportation, communication, energy, health, economic and governmental affairs the most critical component. Through enhanced input/output equipment, lots of electronic devices communicate with each other and expand the Internet of Things (IoT) universe. In parallel to the IoT universe, when we add the universes of the Internet of Services and the Cyber-Physical Systems, we have reached the Industry 4.0, which was spoken first in Germany Hannover Fair in 2011. The moment we add the power of quantum processors to all these theories, perhaps we will arrive at a dizzying pace to the differences we cannot even imagine today.

Basic characteristics of cyber attacks; lack of definition of resources, low cost, low risk for attackers, does not include direct use of violence, can be globally applicable to both international and domestic. So, we can say that the threat is global and every bit of cyberspace is in danger.

As stated in the ISO / IEC 27000 standard, in the present era, since every IT systems are a part of the interconnected world, they became a critical point of every business. For this reason, organizations' information systems and related infrastructures are in need of protection against security hazards. These hazards can be a computer-aided hoax, spying, sabotage, mischief, fire, and flood. In addition, the standard specifies that cyber attacks such as phishing, password theft, eavesdropping, and malware are becoming more challenging and progressively complex in nature [8].

Ralston et al. mentioned that the connectivity of infrastructures to each other and to control systems through cyber network revealed a critical dependency. He also stressed that this is also a major threat to Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCSs) which was previously unknown [9].

Oman et al. notes that abuse of security vulnerabilities in the SCADA system can cause severe outcomes such as loss of services, damage to equipment, financial loss, natural disaster, and possible death of human being [10]. Parallel to that study, IBM report indicates that that the number of cyber attacks or incidents is not important and that only one event may be enough for the organization to make headlines in the newspapers. [11].

According to the above projections, cybersecurity will continue to evolve and be on the agenda of many people as long as cyberspace exists. For this reason, defense methodologies, as well as threats, are developing. Although defense methodologies have evolved, bringing these methodologies to life requires resources as much as the initial investment of IT systems to prevent threats and maintain our system in confidence.

On the basis of the effective use of resources, all security investments should be made within the framework of the objectives of the organizations. For that, it would be more appropriate for organizations to take “only necessary" measures they need about cybersecurity instead of "all" measures. In addition to this, it will also support the effective use of resources to take the necessary measures as needed.

Various standards such as ISO 27000 series, NIST 800 series and COBIT-5 have been developed to ensure risk management and cybersecurity. These standards provide only examples of best practices and experienced frameworks. However, it is not possible to implement a common security application as all IT systems have different risk worlds and the basic function of each IT system varies.

Due to these changes, it would be convenient for each IT system to establish a system of self-management of cybersecurity and risk assessment. The idea expressed herein is the risk universe will determine the probability of damage or loss, the IT system's inventory value and the value of the information processed on it will determine the magnitude of the damage or loss [6].

Although enterprises usually allocate the biggest part of their resources for risks located in the mitigate section, all risks can hardly be covered. Usage of resources for the right risk has a very important role because it is not wise to pay for the risks which never exposure. With the help of KRI monitoring, annual budget for the unrealized risks can be saved. Likewise, the possibility of realization of the risk by using the KRIs can be re-calculated more accurately and the risk mitigation budget can be rearranged accordingly.

Senior management, responsible for the security of information technologies, are those who do not recognize or do not have to recognize these technologies. However, since they are responsible for information technology, they will also need to be aware of, and even want to be in, the process of risk analysis, which directly affects the security of these systems. Many risk analysis methods are not easily able to ensure the involvement of organizational managers. The main reason for this is the mathematical and statistical methods used intensively in the process. As a result, if these methods are not used, the organization may not satisfy the managers today because these tools are very technical for the managers and it is difficult for the organization managers to understand the process of risk analysis [12].

The more risk is mitigated from the risk group, the top management feels the better. However, since the resources are scarce, some of the risks will continue to threaten the IT system. The resource allocated for those risks that can be tracked by KRI is not wasted and is saved unless the risk begins to expose. In this way, sources can be spent only on really realized risks.

CHAPTER 3

COST OF CYBERSECURITY

Ralston et al. notes that cyber attacks are represented by two different metrics. These are monetary loss which represented by dollars and rate of unavailable services [9].

According to the McAfee report, it is estimated that 2% of countries' national income is normal for cyber-attack damage and that when cybercrime and cyber espionage is more than 2% of the country's GDP, companies and communities will find the loss unacceptable and cybersecurity measures to be taken [3].

A critical element of securing IT systems is being able to pay for it. According to the CSI 2010 survey Richardson highlights that there is an extended deviation into more financing of cyber protection, respective to IT systems overall. This does not mean, inevitably, that more resources were given to cybersecurity sections. It is certain that although cybersecurity expenditures are cut down, security investments has to be made according to the threat and value of IT system. [13].

Gordon et al. found that most organizations underinvest in cybersecurity operations, and confirm that “governments around the world are justified in considering regulations and/or incentives designed to increase cybersecurity investments by private sector firms.” There is not enough focus about results of cybersecurity operations and this may be the result of widespread use of cybersecurity frameworks like NIST, ISO/IEC, COBIT, etc. which ease the use of the process. A new procedure which analysis the costs of cybersecurity can be implemented to the frameworks in order to achieve rather broad applicability [14].

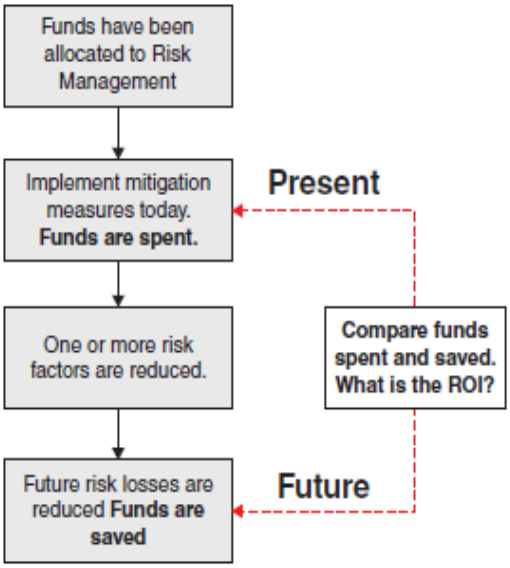


Figure 1: Evaluating an IT System Security Strategy

Studies show that the funds allocated for cybersecurity are especially calculated by Return on Investment (ROI). According to the Bosworth et al. ROI can be calculated when we rate the resource spent for the purpose of risk mitigation with the resources which will be spent in the future (figure-1) [6].

Radzilli Böhme executed an extensive survey of the literature to figure out the connections among the expenditure of cybersecurity and advantages of spending resources for fortifying IT systems. The academic advises using Return on Security Investment (ROSI), that is the difference of spent and avoided costs divided by costs itself. The ratio shows that managing cybersecurity expenditures is matter of science and skill not estimation. [15].

Another study held by Brecht & Nowey. They inspected all techniques practiced to determine and estimate the value of information and IT systems security then classified them into four sections:

- Cost/benefit analysis of cybersecurity (including research on optimal investment),
- Cost of cybercrime,

- Surveys summarizing the actual costs of cybersecurity management,
- Quality cost models.

They claim that effective cybersecurity expenditures include expenditures for purchasing, operating, adapting and redemption, as well as the operational and maintenance costs of purchased security systems and costs of technical personnel who uses these systems. [16].

Although enterprises usually allocate an important part of their resources for risks located in the mitigate section, all risks can hardly be covered. At this point usage of resources for the right risk has a very important role because it is not wise to pay for the risk which never exposure.

With the help of KRI monitoring, annual budget for the unrealized risks can be saved. Likewise, the possibility of realization of the risk by using the KRIs can be re-calculated more accurately and the risk mitigation budget can be rearranged accordingly.

CHAPTER 4

INFORMATION SECURITY RISK MANAGEMENT AND MONITORING

According to the ISO / IEC 27005 standard, a systematic approach to ISRM is required, that is imperative to establish organizational needs related to information security requirements and to set up an effective ISMS. It is stressed that this way should be appropriate for the organization's strategic objectives and culture and should be particularly compatible with long term risk management. All studies about cybersecurity should be arranged adequately, on time and on place when and where just needed. The whole cybersecurity activities must be a part of ISRM. These activities should be covered both in the implementation and operational phases of ISMS. [17]. In other words, it is necessary for an IT system to carry out a risk analysis against the hazards and then it is necessary to take precautions in terms of resources to eliminate the risk list.

Şahinaslan et al. agrees that the assessment of the systems to be defended within the scope of the cyber defense and analyzing risks are anticipated as an important issue in terms of effective usage of available scarce resources. At the point of providing information security, organizations need to determine the cybersecurity risks first, and the existing risks should be taken to an acceptable level according to the organization. After that, organizations should establish a risk methodology in line with their needs before risk assessment of cyber systems safety [18].

In this context, it will be inevitable to conclude the value of the systems possessed and to apply intelligent approaches for allocating defense efforts at these values. In order to be able to determine the value of the systems, it is necessary to assess the consequences of attacks and the real aim of the adversary or aggressor.

In many sources risk analysis practices, qualitative and quantitative calculation methods, risk scenario adaptation, risk list generation techniques are specified. Finally, all calculations are derived from the following form: “Risk = f (Entity, Vulnerability, Threat)”. The function “f” in the form expresses the risk model. This model has three basic inputs, and the output of this function (model) is also a risk value.

At first, the asset value is calculated for situational awareness. Then a list of existing risks is made for the purpose of establishing a full and comprehensive threat analysis. Afterward, the risks are minimized by developing and applying measures. But these are not enough to be safe. Morgan stated that reliable cybersecurity risk list needed to be constantly updated and necessary risk reduction measures should be applied [19]. However, it is hardly possible to be instantly aware of all types of attacks that take place in the whole cyberspace, and also it takes some time to take risk prevention measures against these emerging threats. During this time, although we are aware of the risk, we are vulnerable for a while against this threat because we cannot be able to shut down or disconnect our running IT systems.

On the other end, Takçı et al. emphasize that the assessment of information security risks is rather difficult than other risk assessments because information about the probability and information cost of security risk factors cannot be calculated easily and constantly changing [20]. In addition to Takçı and his colleagues, 20th Global Information Security Survey (GISS) shows that the percentage of institutions which has reporting process of IT cybersecurity events is 63% nevertheless, 89% of institutions aware that protecting procedures of IT doesn't comply with the requirements. [19].

Moreover, all the measures that are considered necessary require additional investment and resources, so senior managers are having difficulty deciding on these issues. There are differences in knowledge between the technical team and the senior managers within the scope of setting up an effective defensive

establishment with limited resources. IT personnel are thinking technically while managers are approaching the issue of income-expenditure. Beling and Crowther stated in their article that many senior managers and executives are afraid to take responsibility in implementing security measures for organizations IT systems because there is a profound gap among managers and technical personnel. Therefore senior management usually miscalculates and misunderstands the status of risk and likelihood of cyber threat. [21]. ISRM should include an appropriate risk assessment and risk mitigation method that can figure out costs and benefits, address stakeholders' concerns, and compatible with legal requirements. Managers and staff must be trained on risks and mitigating measures [17].

CHAPTER 5

KEY RISK INDICATOR (KRI)

5.1 What is KRI?

> Not everything that can be counted counts, and not everything that counts can be counted. Albert Einstein

Today we are obliged to measure everything we want to keep under control. We use metrics to measure. The primary goal of metrics is to quantify data to facilitate insight. As for indicator, it is a variable that can be measured and it can be replaced by the value of correlated factor or quantity [22]. That means where the metric is data, the indicator is information. For example, the number of customer complaints is a metric but the percentage of resolved customer complaints is an indicator. Since these metrics are not enough for themselves, we use indicators to take action.

Monitoring and measuring are the initial actions to be taken when measuring an information system security performance and the effectiveness of the ISMS. When it comes to measuring a large number of metrics for information security, it is difficult to decide which metrics should be measured. This issue is very important because it is not feasible, expensive, and almost not possible to measure too much or incorrect metrics. Key metrics can be used for large quantities of data so that appropriate measurements can be made without adversely affecting these negative aspects [23].

Although slightly different, organizations use three different types of metrics: “risk (exposure) indicators, control effectiveness indicators and performance indicators”. They are explained below [24].

A Risk Indicator is a metric that allows an organization to monitor changes in the level of risk to be able to proceed with its business safely. Risk Indicators provide specific information about the exposure of operational risk level that the institution has at a given time. To provide this information, the Risk Indicator must be in an understandable and apparent relationship with the particular risk that shows the risk it is exposed to. Risk Indicators emphasize action points. In addition, they can be pioneer indicators of risks to be realized. These are usually "forward-looking" or "leading" indicators.

A Performance Indicator is a metric that assesses how an organization performs against targets. A defined target (typically) provides a reference point when evaluating a Performance Indicator metric. These metrics are usually "backward-looking" or "lagging" indicators.

A Control Indicator is a metric that assesses the level of effectiveness of control (or group of controls) applied to reduce or mitigate particular risk exposure. A Control Indicator typically supported by an evaluated threshold or trigger. These control indicators are known as backward-looking or lagging indicators. They are bound to institutions' objectives both in operational and process levels.

If an indicator is selected as an important metric then it is called "key". Such key indicators can reveal information about performance, risk, and control processes. They are also settled and distributed for specific risk owners and responsible divisions to make decisions at each discrete layer.

According to ISACA, "KRIs are metrics capable of showing that the organization is subject or has a high probability of being subject to a risk that exceeds the defined risk appetite" [25]. Ann Rodriguez describes KRI as "a metric permits a business to monitor changes in the level of risk to take action. KRIs highlight pressure points and can be effective leading indicators of emerging risks" [24].

In her study Strachnyi agrees that, although KRIs are not a comprehensive solution for risk management, they are accepted as a valuable instrument in the context of risk management. They are also used to augment the monitoring and mitigation of risks and ease risk reporting [26]. They are related to a specific risk and shows changes in the likelihood or consequence of the risk occurring.

Setting up effective KRIs lies in the understanding clearly the organization's purpose and targets. An effective KRI metric set can give vital information about potential risks that would affect the realization of targets or would reveal the existence of new opportunities.

KRIs are differed because of organizations strategies and objectives. For that, they are unique for every organization. Development and selection of KRIs are based on different parameters like the complication and extent of the organization. The company may operate in a marketplace with extremely regulations, and the focus of the strategy.

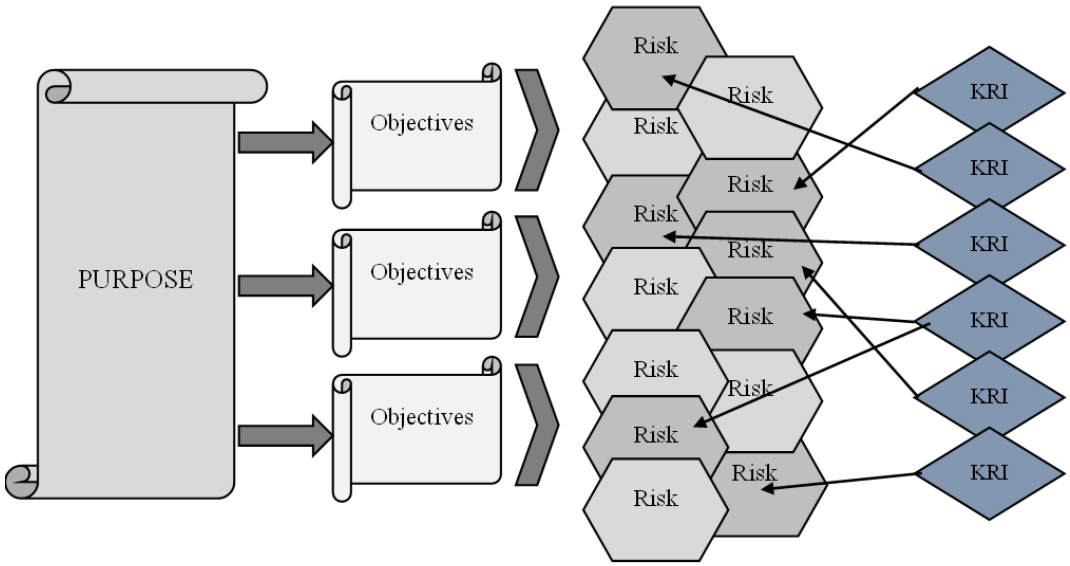


Figure 2: KRI Mapping

The figure-2 illustrates three key objectives that are appropriate for the purpose of the organization. There are various potential critical risks that can affect

one or more of the objectives in relation to the targets. KRIs are linked to critical risks in order to give information to the Information Security Management and Executive Management about the exposure of risk happening. This information may change to an “alarm” about thresholds preselected. With the alarm, Executive Management can decide to bring in the mitigation plan in order to reach the company's goals and to realize its strategy. While some KRIs are linked to only one risk others can be linked to more than one risk.

In an organization a broad group of metrics may be developed to work as risk indicators; however, it is not likely or appropriate to investigate or watching over all sets of metrics. Especially when these sets become a considerable amount, they cannot be controlled anymore. So, what we need to do is to concentrate on only the important indicators which are "key" indicators. KRIs are different from other indicators because they are highly relevant and they predict or indicate key risks with a high probability. This technique facilitates risk management and monitoring.

Using KRIs for monitoring risks can bring the following advantages to the organization:

- With “forward-looking” or “leading” KRIs early warning can be set in order to provide a proactive action.
- With “backward-looking” on risk events, you can still learn from past events.
- As you monitor risk appetite and tolerance you can decide at a point where risk is about to happen and maximize risk-based earnings.
- KRIs give easy and simple warnings so that decision makers and risk managers can decide and take action in real time.
- KRIs help the organizational management keep track of trends in risks. This can help determine areas where more investment may be needed or opportunities may arise [25].

It is not possible to prepare a standard or universal KRI set that can be used in any organization. This is due to the fact that each risk is not the same and that the specific effect ratings for organizations are different. In addition, the measurement frequency of the indicators is another important factor. More useful data will be obtained than the more frequently measured markers [27].

When used properly KRIs also help to prevent False Positives. For example, deviations in bandwidth, protocols, and ports do not always mean an anomaly in organizations network. The root cause may be different like a remote application may attempt to open a normally closed port. So, we can set thresholds and KRIs to monitor bandwidth to avoid wrong decisions.

5.2 How to Develop KRI?

There is no international standard or best practice book published for KRI development maybe because they are designed for risk related to every specific entity's purpose and objectives. In the researches, it is seen that most of the organizations developed their own KRI development procedures to be used in their own risk management. While procedures such as Identification, Selection, Establishment, and Reporting are the same in most of the organizations, other procedures such as Defining Sources of Risks, Planning Risk Mitigation, and Responding developed differently.

Table 1: Matruglio and Tymmons' KRI Develop Procedures

1.	Identify Risk
2.	Define Sources of Risk
3.	Establish KRI

In the aforementioned KRI development processes, Matruglio and Tymmons showed the shortest one at the RIMS Risk Forum presentation in 2014. See table-1 as they showed the way to develop KRIs in three procedures [28].

Table 2: Pleshakova's KRI Develop Procedures

1.	Identify Risks
2.	Selection of Risks
3.	Setting Triggers
4.	Planning Risk Mitigation
5.	Reporting

While Matruglio and Tymmons keep developing KRIs in a simple way and count on three steps Pleshakova describes KRI development process in five procedures as shown in table-2 [29].

Australian Finance Department agrees with Pleshakova for the first two steps but they think reporting procedure has priority on action procedure. With four steps seen in table-3 they develop KRIs, but thresholds or triggering steps are not involved [30].

Table 3: Australian Finance Department's KRI Develop Procedures

1.	Identify Risks
2.	Selection of KRIs
3.	Reporting
4.	Actions

Mouatassim and Ibenrissoul decided another four procedures. As it is seen in table-4 they described management procedure different from others [31].

Table 4: Mouatassim and Ibenrissoul's KRI Develop Procedures

1.	Selection of KRI,
2.	Setting up of alert thresholds,
3.	Management of KRIs,
4.	Reporting of KRIs.

5.3 KRI Properties

In order to control cyber risk management performance, technical teams use many computation methods and metrics. The use of KRIs and risk owners differ according to objective levels and culture of the organization. Chief Information Security Officer (CISO), Chief Risk Officer (CRO), steering board and top management has different risk levels. The effective design of KRIs and their harmonization with the institutions' strategy and objectives, provide a stronger connection with the company's board of directors and senior management. This provides a non-technical perspective of the program and facilitates the control. The main goal of efficient KRI design is to monitor risk-related activities to sense and detect the exposure of risk at a time and implement risk mitigation activities according to the cybersecurity plan to prevent or mitigate the risk.

KRI helps to decrease costs by providing sufficient risk to a point where risk tolerance and risk appetite is balanced. It also ensures how much an organization can endure to a particular risk and determines when and how much the risk-mitigation process will be applied. With KRI the likelihood of the occurrence of the main risk is monitored. The purpose here is to ensure that risk can be taken up to the level determined by the risk appetite. Risk appetite can vary according to the company in which information systems are installed or it can be determined within the risk framework of the organization. In systems where all risks are eliminated, the security policies and applications make the system very hard to operate and

users are expected to pass through a lot of security arrangements. In this case, users tend to be more reluctant to use the system or they will try to make things easier by using security vulnerabilities.

When we follow risks of this Risk Universe, especially the important ones, by using KRI we can give risk prevention or mitigation decisions at any time. What we need to do at this point is to develop thresholds to set the decision time.

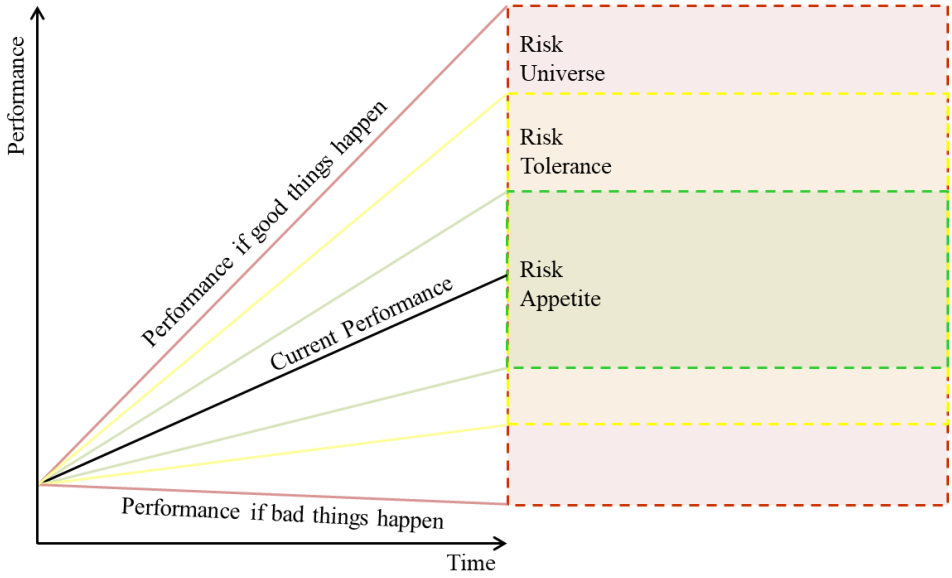


Figure 3: Risk Boundaries

First of those thresholds shows tolerable level in achieving the strategic objectives identified by the senior management of the organization. These risks are approved by the senior management of the organization and include the risks required to achieve the specified objectives. This area is where the risk appetite of the organization is determined. If the risks followed are outside the risk appetite zone, but there is a chance that they can be put below the risk appetite level with the specified mitigation practices, this group is called risk tolerance zone. The risks followed in this region are reduced by applying the risk management procedures determined by the senior management and the risk is reduced below the limit of the risk appetite level. In this regard, senior management gives approval for the use of resources. In addition, monitoring and mitigating procedures related to the ongoing

risk are explained more easily to top management using KRIs. As depicted in figure-3, where the red area shows risk universe, the yellow area shows risk tolerance, and the green area shows risk appetite.

This can be explained with an example as follows: Let’s assume that one of the risks identified by our organization in achieving its strategic goals is that the IT system with vital importance for the organization is partially or permanently disabled. One of the sub-risks that may cause this risk to occur is that the user accounts password with important authorities is not in the standard of security rules defined by the Cybersecurity Officer. It will be very easy to capture passwords that are created outside the standard or not properly protected. However, it is still not possible for all strategic users to use a password in the desired standard. The senior management, who wants to give a certain tolerance in this respect, states that about 5% of the user passwords which have the authority to cause the specified risk may be out of the standard. However, if this ratio exceeds 5% and is between 5% and 10%, then they want all passwords should be checked again, the applicability of existing password standards should be examined and if needed new password standards should be established. With non-compliant passwords reaching 10%-13%, they want passwords that do not comply with the relevant standard to be changed, stop to use the old standard and put the new password standards into effect, to check whether the IT system has abnormal activity, to check the system against known viruses and trojans, and to train related users to avoid duplication.

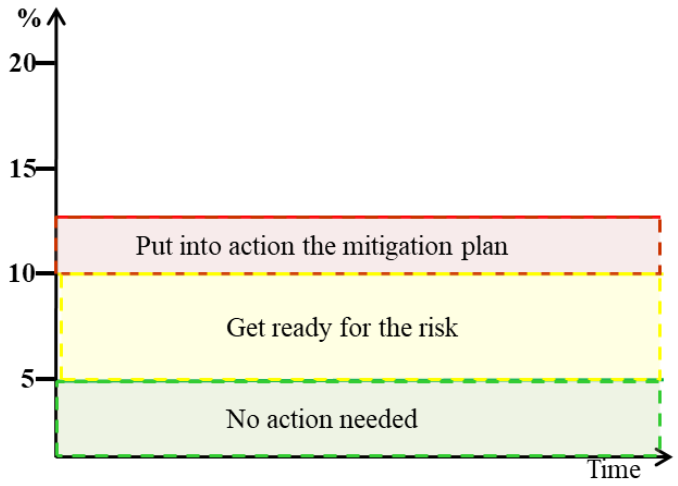


Figure 4: % of High-Risk Assets with Weaker or Non-Compliant Passwords

As depicted in figure-4, in accordance with the instructions of the senior management, KRI is generated as the percentage of non-compliant passwords, and thresholds are selected as between 0% and 5% is the risk appetite, between 5% and 10% is the risk tolerance, and between 10% and 13% is the risk universe. With the help of KRI the exposure of the risk is closely monitored and necessary measures approved by the senior management are put into practice.

Developing good KRI is another important topic. According to Sheldon [32], a well-developed KRI should:

- Be measurable, (e.g., percentage, loss value)
- Has the ability to measure the right thing,
- Has the ability of precise and accurate measurement,
- Has the capability to be validated against empirical evidence within the framework of the metric.

Although there is no standard for good KRI quality, scholars define almost the same features. Mouatassim and Ibenrissoul also asserted the same characteristics of good key-indicators as Sheldon:

- *"Relevance:* Indicators should provide the necessary information about the organization's risk exposure;

- *Measurability:* Indicators should be measured accurately and regularly. Suggested formats are numbers, values, percentages, or ratios. Non-quantitative indicators are subjective and can be misinterpreted;

- *Predictability:* The selected indicators should provide an estimate of changes in the organization's risk profile to take preventive measures;

- *Facility for monitoring:* The data needed to calculate the indicators should be available and affordable. Moreover, these indicators should be relevant and easily interpretable" [31].

In addition to the aforementioned features, The Institute of Operational Risk asserts almost the same desirable characteristics of KRIs as:

- Relevance,
- Measurable,
- Predictive,
- Easy to Monitor,
- Auditable,
- Comparability [27].

On the other hand, there are some specifications that bad KRIs have:

- KRIs are not attached to particular risks.
- KRIs have inadequate or incorrect features i.e. too common.
- Lack of alignment amid the risk, the KRI description and the KRI metric.
- Too many KRIs.
- Difficult to measure.

CHAPTER 6

CURRENT ISRM MODELS

Risk management is the process that IT managers benefit from. It is used to protect the critical systems necessary for the organization to achieve its objectives. The aim of this process is to reduce the risks that the organization will be affected in accordance with the general risk tolerance. Organizations are not expected to eliminate all risks; instead, they try to describe and bring about a tolerable level of risk that will not prevent their strategic goals. The risk management process includes risk analysis, risk evaluation, and risk monitoring sub-processes.

At the point of ensuring information security, organizations should first determine the information security risks by using the mentioned sub-processes, and move to a level that the existing risks will be accepted by the organization. Organizations should also establish a risk methodology in line with their needs before conducting an information security risk assessment.

Within the scope of the thesis, only internationally accepted and practically approved Information Security Risk Management Standards evaluated as the risk methodology. These standards should certify the organizations which establish, implement and document the process of mentioned standards.

Within the scope of the available resources in the literature, the standards that may be included in the study have been examined, and the ISO / IEC 27000 series standards published by the International Organization for Standardization (ISO), which is a non-governmental international organization, and NIST 800 series ISRM documents that are required to comply with USA government IT systems are selected as appropriate standards. For this reason, ISO / IEC 27001 and NIST 800

series were examined in this study as comprehensive and up-to-date ISRM standards.

6.1 ISO/IEC 27005 Risk Management Model

The ISRM Process stated in ISO/IEC 27005 standard starts with the establishment of the context where organizations' IT systems value (including human resources and the knowledge inside), goals and objectives included. In this process, Risk Evaluation Criteria are developed. These criteria include the strategic value of IT system, critical personnel and information, legal requirements, the operational importance of CIA triad and finally stakeholders' considerations. After criteria tree formed, Risk Acceptance Criteria should be developed according to organizations' goals, objectives, policies, and senior managements' aim. These criteria may include multiple thresholds like KRI process. Those mentioned criteria, scope, and boundaries of information security risk management are subject of senior management.

After calculating the value of the system to be protected, Risk Assessment comes. In the Risk Assessment process, there are three sub-processes: "Risk Identification, Risk Analysis, and Risk Evaluation".

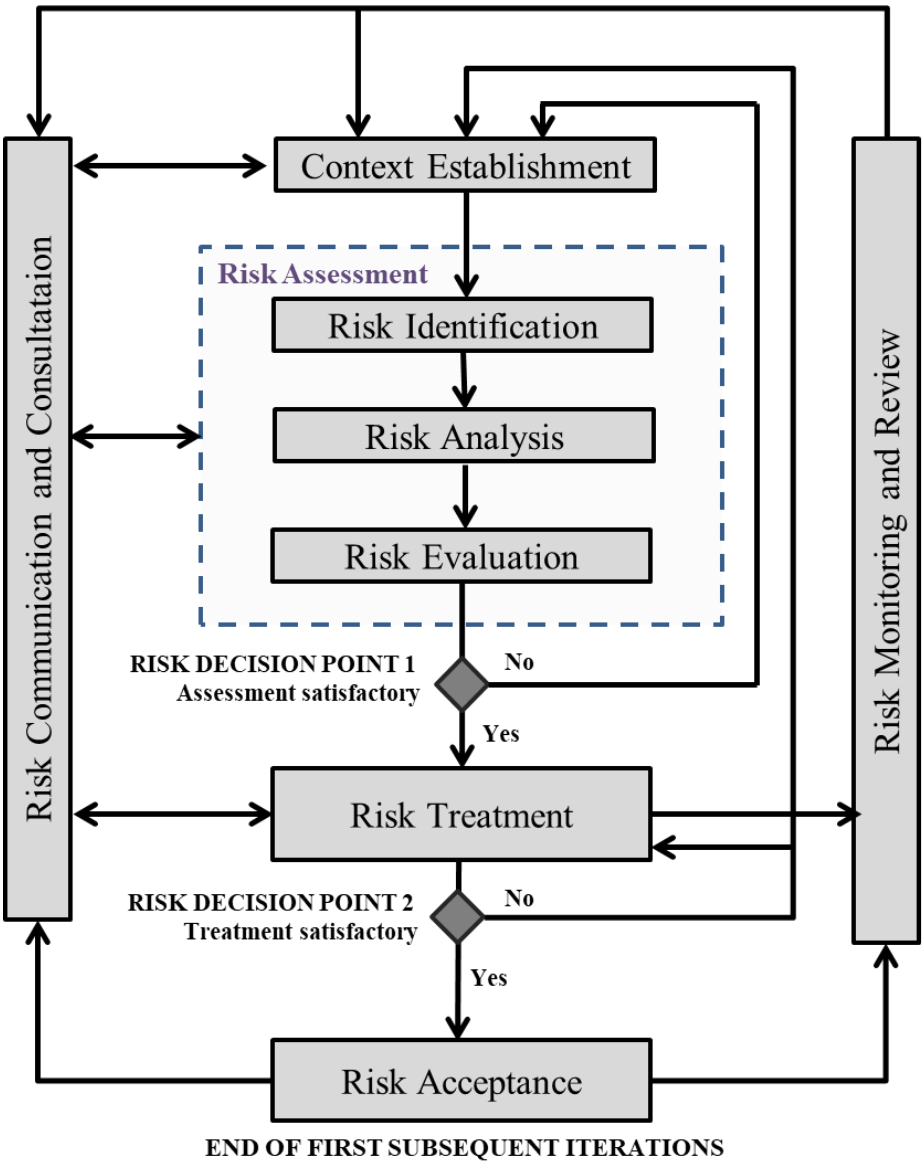


Figure 5: Illustration of the ISO/IEC 27005 ISRM Process

The purpose of risk identification is to determine what could happen to cause a potential loss and to gain insight into how, where and why the loss might happen. For this purpose, the first thing to do is to list all assets to be risk managed. Then the asset list is developed, threats should be listed. Then Identification of Existing Controls comes. In this sub-process list of existing and planned controls are established. After that standard says vulnerabilities concerning assets, threats and controls should be listed. The last job of Risk Identification is documenting a list of

scenarios with their consequences related to assets. Figure-5 illustrates the ISRM Process as stated in ISO/IEC 27005 standard.

In Risk Analysis sub-process Qualitative and Quantitative analysis methodologies are used to assess consequences, the incident likelihood and to determine the level of risk. The first thing for analyzing risks is to develop a list of assessed consequences of an incident scenario expressed concerning assets and impact criteria. Secondly, the likelihood of the incident scenarios is assessed. And finally, after risk levels determined the list of risks with value levels assigned is evolved.

The third sub-process of the Risk Assessment is Risk Evaluation. In this process, estimated risks are compared with the risk evaluation criteria which are consistent with the defined ISRM context.

When Risk Assessment is completed, the ISRM Process reaches the first decision point. At this point, if the assessment is not satisfactory, the process begins with the Context Establishment again. If the assessment is found satisfying, then the Risk Treatment plan is executed. After Risk Treatment plan is completed, the process reaches to the second decision point. At the second decision point, if the treatment is not satisfactory then the process begins with the Context Establishment again just like the first decision point. If the treatment is found satisfactory then there is no risk to worry or the residual risk can be accepted.

While these processes are performed, communication with the decision makers and other stakeholders are always established. While all these processes are realized new assets with their values, new threats, change in requirements, new or increased vulnerabilities or incidents can be unveiled. Therefore, the Risk Monitoring and Reviewing Process is always active in detecting new events.

6.2 NIST 800 Risk Management Model

To ensure the security of official information systems used throughout the country, U.S. National Institute of Technology (NIST) published a cyber framework. Everyone who wants to work in relation to U.S. IT systems has to comply with this framework. The risk management process in the NIST 800 framework consists of two main sub-processes. These are risk analysis and risk control processes. The risk analysis process exposes the assets in the system of activity, the vulnerabilities in the assets, the threats that can exploit the vulnerabilities, and the security measures used to protect the IT system.

The relevant procedures for risk analysis and risk practices are set out in the frameworks NIST 800-30 rev.1 Guide for Conducting Risk Assessments, NIST 800-37 rev1 Guidelines for Federal Information Systems and NIST 800-39 Managing Information Security Risk.

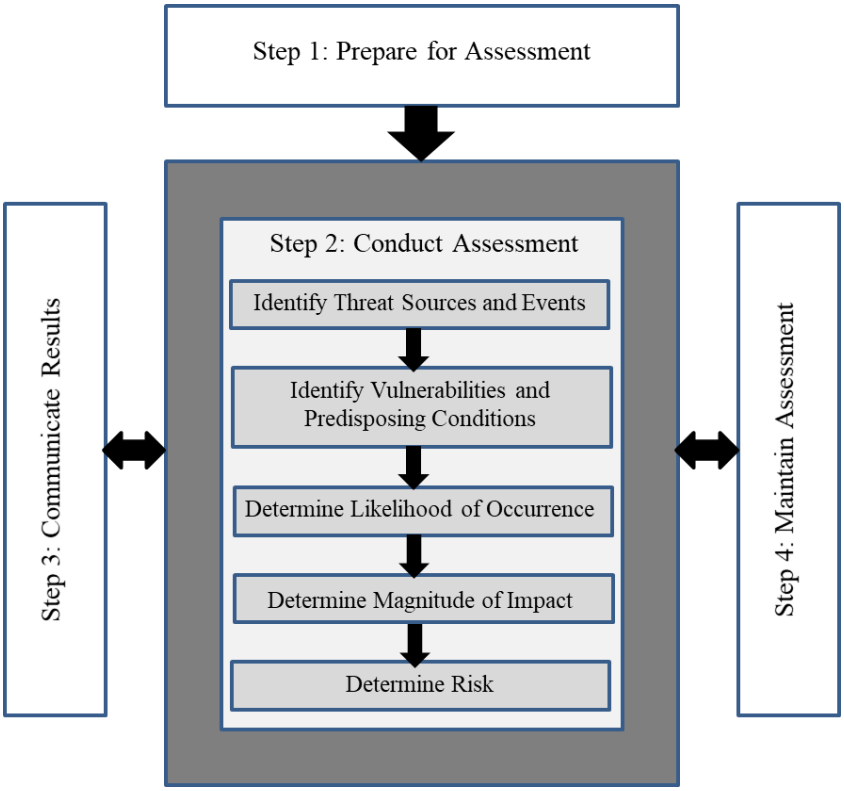


Figure 6: NIST 800-30 (rev.1) Risk Assessment Process

As seen in figure-6, NIST 800-30 rev.1 Guide for Conducting Risk Assessments has a systematic approach for assessment of the risks that can affect the IT systems of organizations is performed [33].

- STEP-1: Prepare for Assessment
- STEP-2: Conduct Risk Assessment
- STEP-3: Communicate and Share Risk Assessment Information
- STEP-4: Maintain the Risk Assessment

STEP-1 Prepare for Assessment: The objective of this step is to establish a context for the risk assessment. In this step the following tasks are executed:

- Identify the purpose of the assessment,
- Identify the scope of the assessment,
- Identify the assumptions and constraints associated with the assessment,
- Identify sources of threat, vulnerability, and impact information,
- Define the risk model, assessment approach, and analysis approach.

STEP-2 Conduct Risk Assessment: The objective of this step is to produce the risk list. In this step the following tasks are executed:

- Identify threat sources,
- Identify threat events,
- Identify vulnerabilities,
- Determine the likelihood,
- Determine the adverse impacts,
- Determine information security risks.

STEP-3 Communicate and Share Risk Assessment Information: The objective of this step is to ensure that the senior management or decision makers have the appropriate risk-related information. In this step the following tasks are executed:

- Communicate the risk assessment results,

- Share information.

STEP-4 Maintain the Risk Assessment: The objective of this step is to keep the specific knowledge of the risk up to date. In this step the following tasks are executed:

- Monitor the risk factors
- Update the components of the risk assessment.

NIST 800-39 Managing Information Security Risk Standard is accepted as the flagship security information document NIST developed. The purpose of this guide is to provide holistic information security risk management. It provides structural, but flexible risk management approach.

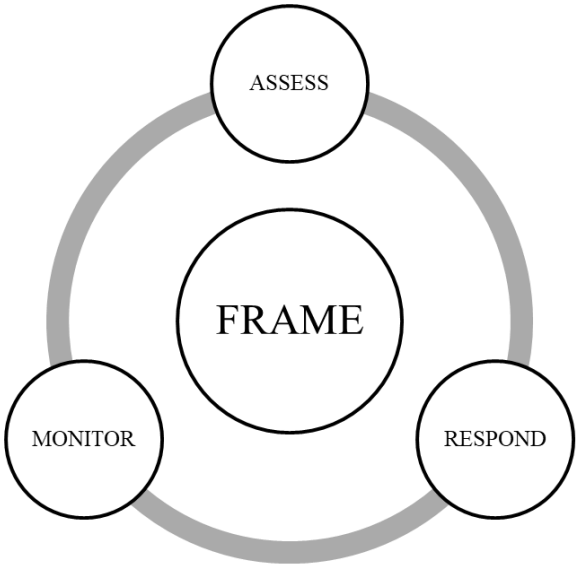


Figure 7: Risk Management Process of NIST 800-39

NIST 800-39 guide allocates the risk management in four components (figure-7). The first component of risk management describes how organizations develop risk context or frame risks. The purpose of the risk framing component is to develop a risk management strategy. In order to establish a context risk, assumptions, risk constraints, risk tolerance, and priorities are identified [34].

The second component of risk management describes how organizations assess risk. The purpose of the risk assessment is to identify threats, vulnerabilities, harm, and the likelihood. At the end of this component determination of risk is obtained. In order to support risk assessment component organizations are expected to identify:

- The tools, techniques, and methodologies used to assess risk,
- The assumptions,
- The constraints,
- Roles and responsibilities,
- How risk assessment information is collected, processed, and communicated throughout the organizations,
- How risk assessment is conducted,
- The frequency of risk assessment,
- The dissemination of threat information.

The third component of risk management describes how organizations respond to risk. The purpose of this component is to provide a consistent and organization-wide risk response.

The fourth component of risk management describes how organizations monitor risk over time. The purpose of this component is to verify that planned risk response measures are implemented, to determine the effectiveness of risk response measures, and to identify risk impacting.

Figure 8: Multitiered Organization-Wide Risk Management

In order to implement those components into an organization, NIST 800-39 guide advises a three-tiered approach (figure-8). Three-tiered approach manages risk at the organization level, mission/process level, and information level [34].

The first component, Tier 1, addresses risk from the organizational perspective. This part provides the context for all risk management activities and affects other activities carried out at Tier 2 and Tier 3. Tier 1 provides a prioritization of which drives investment strategies and funding decisions. The section of common controls, the provision of guidance from the risk executive to authorizing officials, and the establishment of the order of recovery for information systems are examples of Tier 1 activities.

Tier 2 deals with the risks from a mission/business perspective and is informed by the risk context, risk decisions, and risk activities at Tier 1. Defining the mission /business processes needed to support the missions and business functions of organizations, prioritization the mission/business process, defining the types of information, incorporating information security requirements and establishing enterprise architecture are examples of Tier 2 activities.

Tier 3 deals with the risks from an information system perspective and is guided by the risk context, risk decisions, and risk activities at Tier 1 and 2. Categorizing information systems, allocating security controls, managing the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls are examples of Tier 3 activities.

In order to apply those frameworks mentioned above, NIST developed 800-37 Risk Management Framework for Information Systems and Organizations (rev.1). It is developed:

- To ensure information security risks are consistent with the mission/business objectives and risk strategy,
- To ensure information security requirements are integrated into the organization's architecture,
- To support security authorization decisions,
- To achieve more secure information systems through the implementation of appropriate risk mitigation strategies.

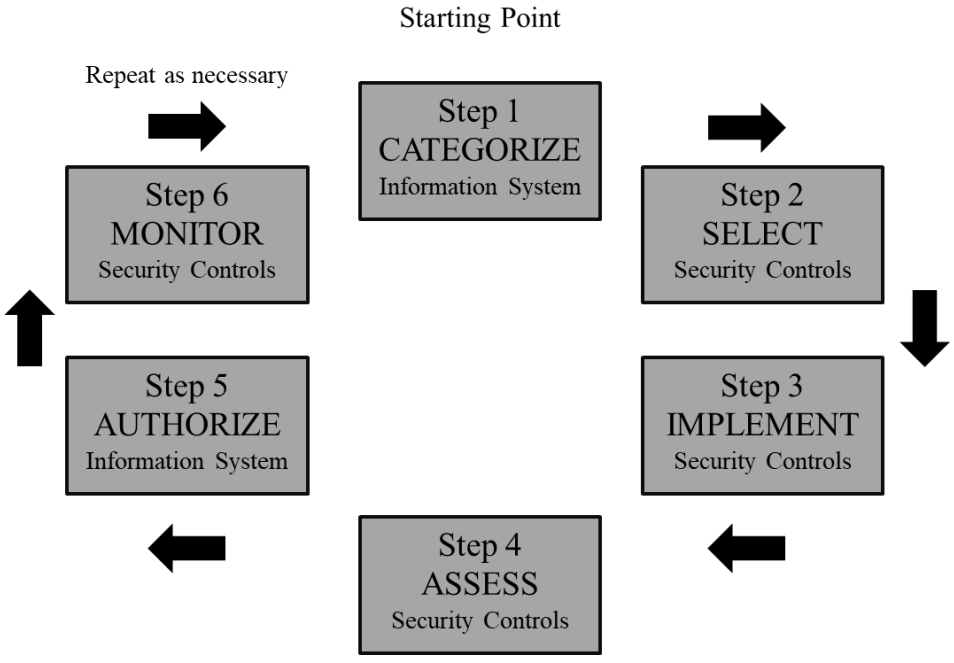


Figure 9: NIST 800-37 rev.1 Risk Management Framework

In addition to the frameworks NIST 800-30 and NIST 800-39, NIST 800-37 rev.1 applies 6 staged Risk Management Framework (figure-9) [35]. Those stages are explained below:

STEP-1 Categorize: In this step, all the information system itself and information inside this system are classified according to the impact analysis. Security categorization helps to reflect the organization's risk management strategy and to describe the characteristics of the information system adequately.

STEP-2 Select: In parallel with the security categorization, a set of baseline security controls are developed. Within security control set common controls (inherited by one or more organizational information systems) for organizational information systems are identified and documented into a security plan. In addition, a strategy for the continuous monitoring of security control effectiveness is developed. At last the security plan is reviewed and approved.

STEP-3 Implement: This step describes the implementation and documentation of security controls selected in step-2.

STEP-4 Assess: Implemented security controls are assessed. In agreement with the Comprehensive Assessment Plan, an independent assessor fulfills security control assessment. The necessary remediation actions are taken by the organization.

STEP-5 Authorize: Information system operations are authorized based on a determination of the risk. After a Plan of Action and Milestones reflecting organizational priorities developed, appropriate authorization package with all key documents is shaped. Once the Security Assessment Report, Plan of Action and Milestones have been reviewed by the Authorizing Official, the system is authorized and the risk is accepted by the Authorizing Official.

STEP-6 Monitor: In this last step security controls in the information system are monitored on an ongoing basis. In addition, actual changes of information

system and its environment of operation are monitored, the technical, management and operational security controls are assessed. With results security plan is updated.

In both ISO/IEC 27000 and NIST 800 series ISRM standards, it is clear that KRI methodology is not used.

CHAPTER 7

PROPOSED MODEL FOR IMPLEMENTATION OF KRI INTO ISRM STANDARDS

In the proposed ISRM model, new sub-processes are added to enhance the Risk Monitoring and Review processes such as:

- Developing Key Indicator Criteria,
- Risk Evaluation,
- Defining Key Indicators,
- Selection of Key Risk Indicators,
- Continuous Monitoring of KRIs,
- Deciding & Reporting,
- Risk Response.

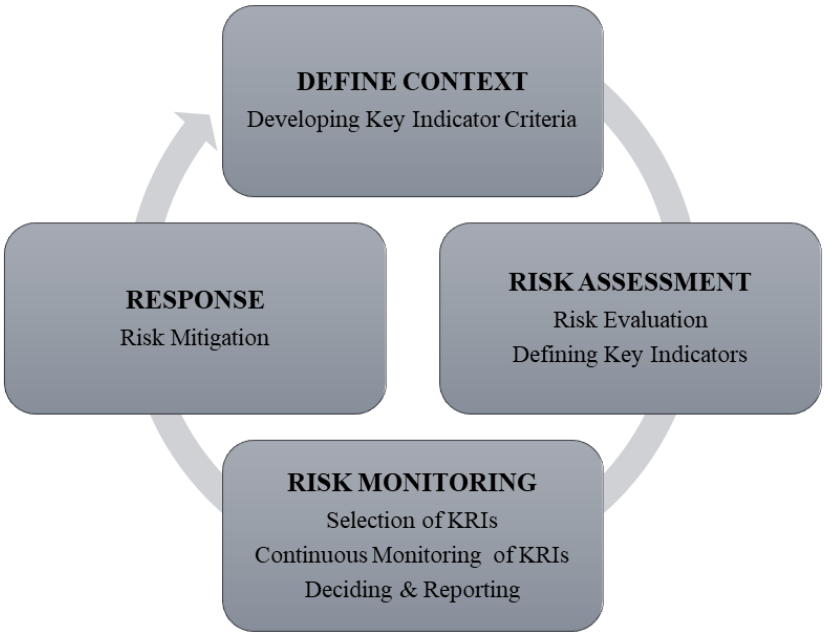


Figure 10: Proposed Model for Implementation of KRI into ISRM Processes

As depicted in figure-10, in the proposed ISRM model, unlike other NIST and ISO / IEC models, risk mitigation and monitoring are carried out by KRIs. The aim here is to prevent the spending of resources for the risks which have not happened yet. In order to achieve this goal, Key Indicator Criteria is defined in the Define Context Phase. Then, according to the Key Indicator Criteria, Key Indicators defined during the Risk Assessment Phase before Key Risks and KRIs are developed.

One of the most important parts of the Proposed Model is the Risk Monitoring & Review Process. Key Risks and KRIs are mapped in this process with risks and KRIs are started to be monitored. According to the alarms to be established by KRIs, status is reported to both Risk Response Supervisor and Senior Management according to Risk Appetite and Risk Tolerance Levels. In the Risk Response Process, risk treat, avoid or transfer is performed by the related unit like CISO. The Residual Risk is accepted and reported to senior management again. Planned measures are put into practice after risks start to emerge. Therefore, the resources allocated for unrealized risks are saved.

7.1. Define Context (Developing Key Indicator Criteria)

Cybersecurity risk management starts with context defining. During process, while goals, objectives, and context are developed, Key Indicators Criteria are established in addition to the basic criteria. Usually, in ISRM standards, Context Establishment process outputs are: The specification of basic criteria, the scope and boundaries, and the organization for the ISRM process.

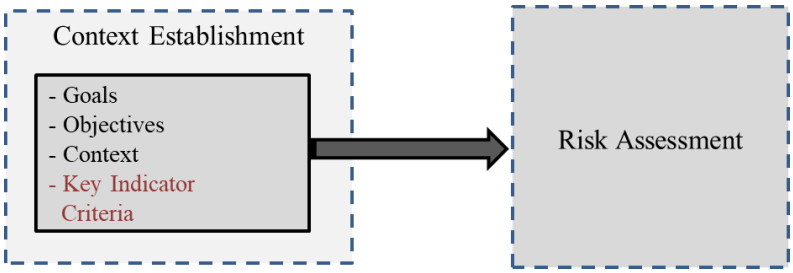


Figure 11: Define Context Process

On the other hand, as figure-11 shows, in the proposed model Key Indicators Criteria is the additional output of the Define Context process.

Organizations may develop at a very significant number of criteria according to their purposes and objectives, but it is neither possible to analyze nor feasible to monitor all sets of metrics. Key Indicators Criteria should be developed for controlling the organization's performance and risks considering following KRI criteria basics:

- A key indicator should be relevant to what is being monitored.
- A key indicator should be measured at a high level of precision and repetition.
- A key indicator should provide sufficient information to understand the exposure levels that the indicator relates to.
- A key indicator should be easy to verify.
- A key indicator should be simple and relatively cost-effective.
- A key indicator should be easy to interpret, understand and monitor.

Research by Davies et al. supports that the ideal features of KRIs are:

- Effective in tracking the risk,
- Comparable within and outside the organization,
- Practical and easy to use [36].

Table 5: Criteria for good KRIs.

EFFECTIVENESS	**COMPARABILITY**	**EASE OF USE**
Indicators should; - Apply to at least one specific risk and one business function or activity - Be measurable at	*Indicators should;* - Be quantified as an amount, a percentage, or a ratio - Be a reasonably precise and definite quantity	*Indicators should;* - Be available reliably on a timely basis; - Be cost-effective to collect; and - Be readily understood

specific point in time - Reflect objective measurement rather than subjective judgment - Track at least one aspect of the loss profile or event history, such as frequency, average severity, cumulative loss or near-miss rates; and - Provide useful management information	- Have values that are comparable over time - Be comparable internally across businesses - Be reported with primary values and be meaningful without interpretation to some more subjective measure - Be auditable; and - Be identified as comparable across organizations (if in fact they are)	and communicated

Table-5 provides some criteria for assessing indicators coherent with these three features [36].

7.2. Risk Assessment

In the proposed implementation model, the Risk Assessment Process has four sub-process named Risk Identification, Risk Analysis, Risk Evaluation, and Defining Key Indicators. Among those sub-processes, Risk Identification sub-process and Risk Analysis sub-process are the same as the other ISRM processes.

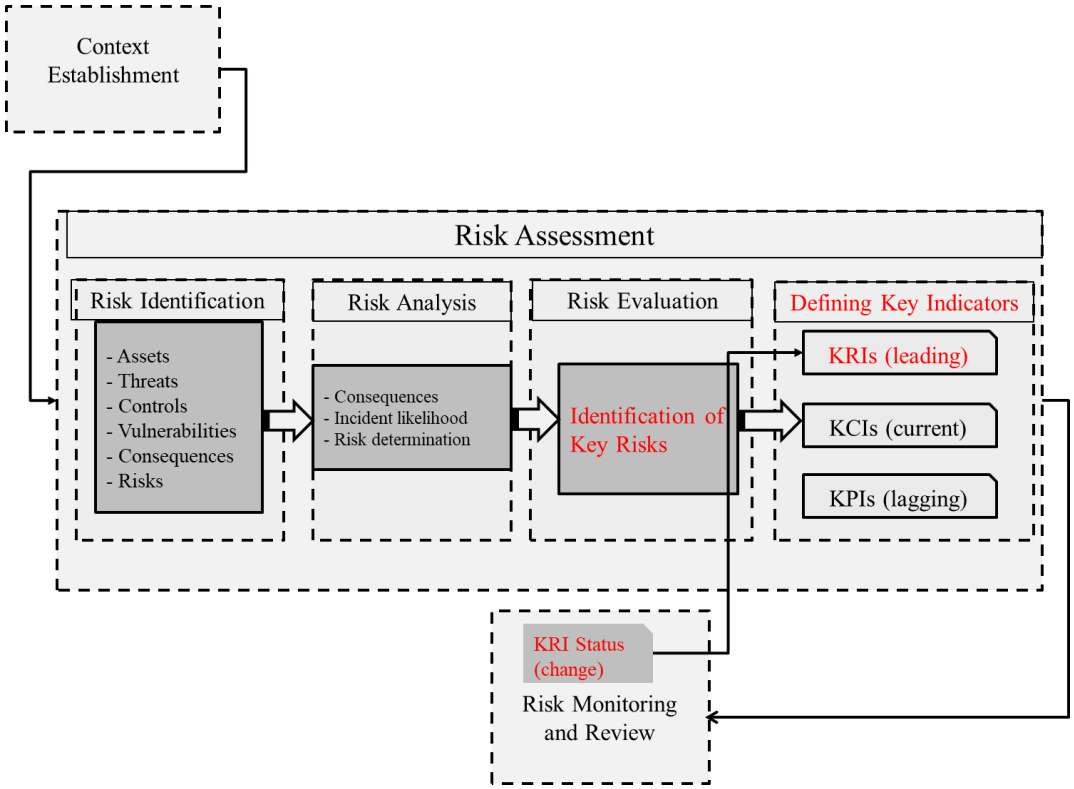


Figure 12: Proposed Risk Assessment Process

During the Risk Assessment Process assets, threats, existing controls, vulnerabilities, and consequences are identified. Incident likelihood assessment, consequences assessment and level of risk determination are also developed in the same context. The difference is the proposed model has new sub-processes named Identification of Key Risks and Defining Key Indicators (figure-12).

7.2.1. Risk Evaluation

Risk Evaluation process generally has a list of risks with value levels assigned, risk evaluation criteria and risk acceptance criteria as input. This process compares the level of risks against risk evaluation criteria and risk acceptance criteria. Decisions are mainly based on the acceptable level of risk. In addition, consequences and likelihood are considered as well. As a result, with the help of incident scenarios and risk evaluation criteria, a list of prioritized risks is obtained.

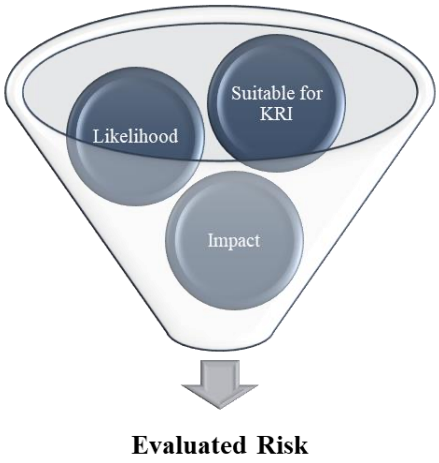


Figure 13: Three Dimensions of KRI Embedded Risk Evaluation

In the proposed model, the availability of the risks for being monitored by KRIs is third dimension (figure-13). According to this evaluation, we could easily develop key risk list harmonized with KRI conformity. To ensure that, Key Indicators Criteria is used in addition to risk evaluation criteria and risk acceptance criteria as input. With the help of Key Indicators Criteria, Key Risks are identified in the Risk Evaluation sub-process. Key risks are risks which are suitable to be monitored with key indicators. If a risk in the risk list has relevant, measurable, predictive, auditable, comparable and traceable indicators than it is a Key Risk.

Table 6: Proposed Model Risk Evaluation Sub-Process

RISK EVALUATION		
INPUTS	**ACTIONS**	**OUTPUTS**
Risk list with value levels	Compare the level of risks	Prioritized risk list
Risk evaluation criteria		Key risk list
Risk acceptance criteria	Identify key risks	
Key indicators criteria		Key indicators list

At the end of this sub-process, we have prioritized risk list, key risk list and key indicators list as output (table-6). Key Risk List is the input of a new sub-process named “Defining Key Indicators” under the process of the Risk Assessment process.

7.2.2. Defining Key Indicators

Defining Key Indicators is a new sub-process in the proposed model. It comes after Risk Evaluation sub-process.

Any kind and piece of data or information can be regarded as an indicator. However, too much or too little metric usage is not appropriate for the organization because it would be very hard to put meaning in such big data or insufficient data. Accordingly, the organization must allocate a wide range of specific metrics that are used to create very specific features to be adopted as Key Indicators and to show changes in exposure levels. Every piece of data can be regarded as indicator but every indicator may not be revealed. Finding out an indicator usually depends on CISO’s experience and ability.

Table 7: Proposed Model Defining Key Indicators Sub-Process

DEFINING KEY INDICATORS		
INPUTS	**ACTIONS**	**OUTPUTS**
Key risk list	Identify key indicators	*Key Risk Indicators*
Key indicators list		Key Control Indicators
Key indicators criteria		Key Performance Indicators

During Defining Key Indicators sub-process Key Risk List, Key Indicators List and Key Indicators Criteria are used as input. With these inputs, key indicators are identified.

In the Defining Key Indicators sub-process, outputs are divided into three groups as Key Risk Indicator, Key Performance Indicator, and Key Control Indicator. If the indicator is a leading indicator, then it is used as a Key Risk Indicator. If the indicator is a lagging indicator, then it is used as a Performance Indicator or Key Control Indicator (table-7).

7.3. Risk Monitoring and Review

In the Risk Monitoring and Review process, the proposed ISRM model claims to use KRIs to enhance monitoring, to use only necessary resources and to minimize false positives. Therefore, the Risk Monitoring and Review process firstly focuses on Key Risk List which is the output of Risk Evaluation sub-process, and Key Risk Indicators List which is the output of Defining Key Indicators sub-process.

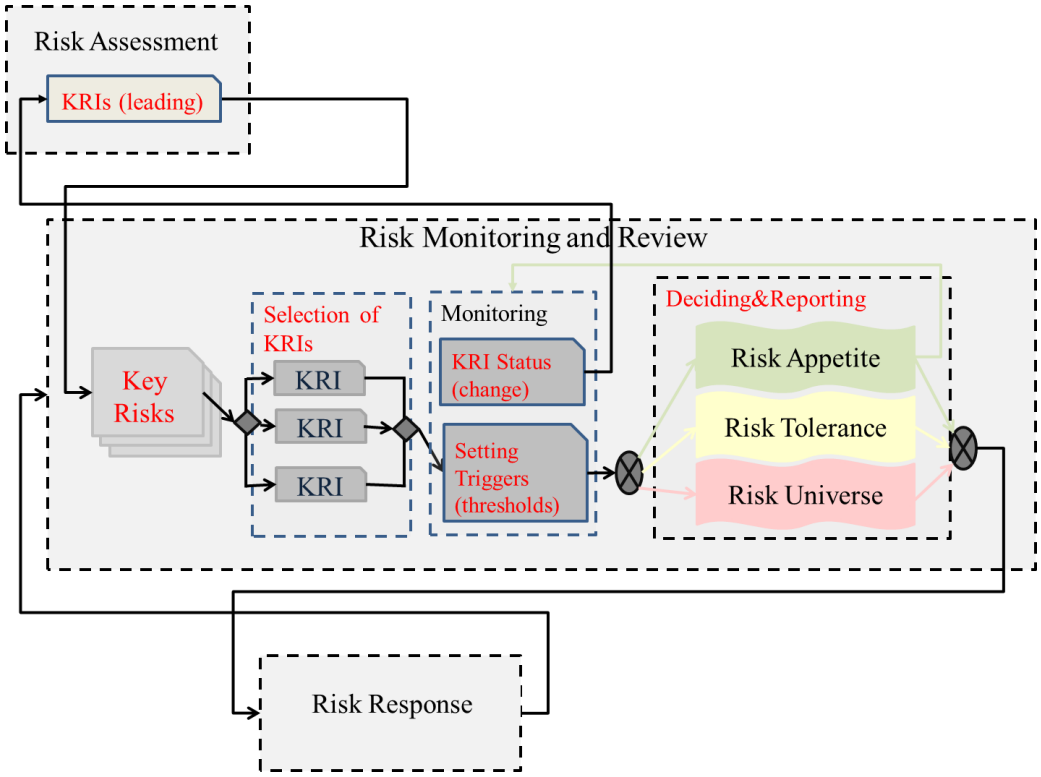


Figure 14: Risk Monitoring and Review

In the proposed KRI implementation model, the Risk Monitoring and Review Process has three new sub-processes named as Selection of KRIs, Continuous Monitoring of KRIs, and Deciding and Reporting (figure-14).

7.3.1. Selection of KRIs

In Selection of KRIs sub-process, it is necessary to select the KRIs that are measurable, meaningful and predictive. And also risk indicators selection should be balanced. In her study, Pleshakova advises that usually it is the best way to start selection simple and to ensure that the selected key risk indicators drill down to the root cause of the risks [37].

The selection of KRIs to be monitored is usually done in two approaches; top-down or bottom-up. During the top-down approach, KRIs are selected by senior management, which takes into account the strategic goals of the organization. On the other hand, during the bottom-up approach, KRIs selected by managers operating in the executive field of the organization. In both cases, the goal is to meet the most important information needs that each level requires to achieve its strategic goals.

It will not be true to say that one of these two approaches is better than the other. The top-down approach will make it easier for senior management to understand the issues of key risks, as well as allow more convenient resources to be allocated for procedures to be applied against risks. On the other hand, with the bottom-up approach, managers operating in the executive field can select indicators which are most relevant to their specific situation. When examining the existing applications, it is seen that the organizations apply a mixed method combining both approaches, which is determined as the best approach.

While senior management is executing a top-down method, they can choose indicators vertically (according to functions) or horizontally (according to organizational structure) depending on the organizational structure of the organization. Top-down indicators should meet the following criteria:

- Depending upon the level at which selected; indicators should cover the operational risk profile of the section or division, business method;
- The indicator should cover a meaningful and understandable metric set which facilitates integration across relevant business entities, product or service areas, and business lines at the relevant level of management;
- They should be imposed by senior management and must be reported on, without choice.

On the other hand, the selection process for bottom-up indicators should consider:

- To ensure that indicators can facilitate the ongoing monitoring of identified risks and controls;
- The results of any regulatory examinations or audit findings should be taken into account in defining and development of indicators in order to help facilitate the rectification of any control or monitoring deficiencies;
- All new processes should be identified as the indicator to monitor and manage the operational risk during the implementation phase;
- The views of the appropriate risk owners (e.g. the relevant department managers or business line managers) or Operational Risk Manager, should be considered;
- Any experience or insights that have been provided by recent loss events (for example in terms of the identification of significant new indicators);
- Changes in the cyber world which might mean that certain indicators become more important. [27]

7.3.2. Continuous Monitoring of KRIs

During Continuous Monitoring of KRIs sub-process, thresholds are determined to monitor relative indicator. To identify thresholds and to monitor metric changes, the Key Risk List and Selected KRIs are used as input. Those mentioned thresholds are formed according to organizations strategic goals, objectives, IT systems' context, and senior management's decisions.

Table 8: Continuous Monitoring of KRIs Sub-Process

CONTINUOUS MONITORING of KRIs		
INPUTS	**ACTIONS**	**OUTPUTS**
Key risk list	Identify thresholds	Green Alarm
		Yellow Alarm
Selected KRIs	Monitor metric changes	Red Alarm

The outputs of Continuous Monitoring of KRIs are green alarm, yellow alarm and red alarm (table-8). If any metric is changed in KRIs, then it is interpreted as green, yellow or red. If the change is within the limits of risk appetite, then the alarm level is set to green which means no action is required. If the metric volume change is upper than green and lower than red level, then it is set to yellow which means ready to take action for the risk because it is probable that risk to be realized. At last, if the metric volume is bigger than yellow, it is set to red which means putting the mitigation plan into action immediately because the risk is happening.

7.3.3. Deciding & Reporting

It is certain that one of the goals of a strong KRI program is to improve decision-making within the organization. An organization has a set of stakeholders that interact with measured metrics which show changes in risk and control levels. Differences in how KRIs are presented are directly related to the purpose of the stakeholder group. The Cybersecurity Officer must have the most complete and detailed set of KRIs to manage progress and continually improve the security of information. Board members and senior management need to understand inherent and residual cybersecurity risks, as well as control costs associated with cybersecurity. To understand these metrics, the cybersecurity risk must have a clear relationship with the organizational strategy and organizational risk appetite, because that is how the inherent risk will be seen [2].

In Deciding & Reporting sub-process, the alarm is generated according to the levels mentioned above. The alarm is reported to the senior management to acknowledge them about the actions carried out. At this point, there is no need for permission of senior management because all activities are preplanned and endorsed by senior management while key risks are defined. Depending on the alarm level, risk response process is activated.

7.4. Risk Response (Risk Mitigation)

During the Response process, risks are at first mitigated to an acceptable level of Risk Tolerance then, residual risks are accepted. The aforementioned Key stakeholders collaboratively decide what the risk response method will be. While deciding, trigger or threshold points are determined based on inputs such as context, IT system itself, business type, etc.

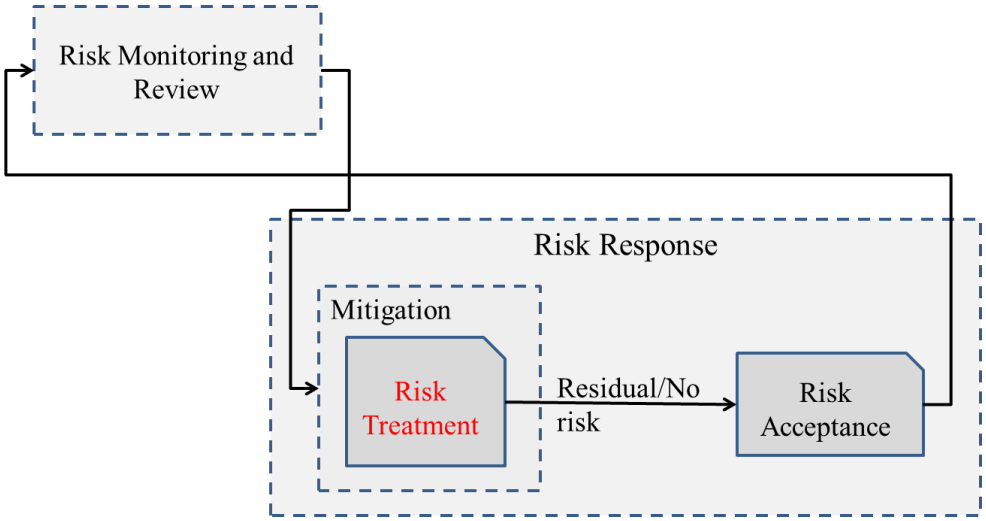


Figure 15: Risk Response

Risk mitigation method reduces the probability of occurrence and/or impact of the risk. This process includes all policies and measures to decrease the probability of occurrence and impact of the risk to be within acceptable threshold limits. By applying, removing or changing security controls, the level of risk is

modified so that residual risk can be reassessed as being acceptable (figure-15). Mitigation has three functions: Treat / Avoid / Transfer.

Table 9: Risk Response Sub-Process

RISK RESPONSE			
INPUTS	**ACTIONS**		**OUTPUTS**
Green Alarm	Treat Avoid Transfer	Accept	Responded Risk Report
Yellow Alarm			
Red Alarm			

Treat: When KRI's alarm the exposure of the risk monitored, the security measures specified in the security plan are implemented (table-9). The exposure level must be above the Risk Appetite and Risk Tolerance levels. The implemented measures aim is to reduce the risk below the level of Risk Tolerance.

Avoid: When the risk alert from monitored KRIs alarms above the limits of Risk Appetite and Risk Tolerance and the risk cannot be treated, the Avoid function is used. In order to avoid the risk, the necessary applications specified in the security plan are processed. With this function, necessary practices are performed for the removal of risk from Risk Universe.

Transfer: When the risk alert from monitored KRIs alarms above the limits of Risk Appetite and Risk Tolerance and the risk is neither mitigated nor avoided, the Transfer function is used. With this function, the risk which KRI shows the exposure of is not removed from the Risk Universe. Instead, its responsibilities of mitigation and the harm transferred to the third parties.

Risks that are mitigated or eliminated by risk mitigation are considered Residual Risks. Accepted risks are transferred to the Risk Monitoring and review process to be monitored again. In this function, the necessary information for Key Risks, KRI selection, and threshold selection are produced. This information is

used to develop Responded Risk Report. Responded Risk Report is used to update Risk Appetite, Risk Tolerance, and Risk Universe.

CHAPTER 8

COMPARISON OF RISK MANAGEMENT MODELS

The ISO / IEC 27000 series and the NIST 800 series ISRM frameworks were compared in the 17 functional areas with the proposed KRI integrated ISRM model. These areas were developed to make the ISRM models more effective, to save budgets, to monitor and to response risks easily.

In the study ISO/IEC 27001, ISO/IEC 27005, NIST 800-30, NIST 800-37, NIST 800-39, and NIST 800-137 standards were compared with the proposed KRI integrated ISRM model. Comparison table of ISO/IEC 27000 series and proposed KRI integrated ISRM model can be seen in APPENDIX A, NIST 800 series and proposed KRI integrated ISRM model can be seen in APPENDIX B and comparison of all related standards and proposed KRI integrated ISRM model can be seen in APPENDIX C.

Table 10: Proposed Model vs ISO/IEC 27000 and NIST 800 Frameworks

	FUNCTION	NIST 800 Series	ISO/IEC 27000 Series	Proposed Model
01.	Using metrics established by the organization	✔	✔	✔
02.	Collecting, correlating and analyzing ALL security related information	✔	Ⓟ	✔
03.	Collecting, correlating and analyzing KEY security related information	✕	✕	✔
04.	Collecting and analyzing the data regularly and as often as needed	✔	✔	✔
05.	Using sample metrics or data	Ⓟ	✕	✕
06.	Collecting and analyzing the KEY metrics continuously	✕	✕	✔
07.	Establishing RISK APPETITE	✕	✕	✔
08.	Acting according to the RISK TOLERANCE (risk acceptance criteria)	Ⓟ	Ⓟ	✔
09.	Establishing RISK UNIVERSE	✕	✕	✔
10.	Defining, selecting and monitoring risk indicators/factors	Ⓟ	✕	✔
11.	Authorizing CISO to determine whether to conduct risk response in accordance with organizations risk tolerance	✔	✔	✔
12.	Responding according to the exposure of the risk	✕	✕	✔
13.	Having risk response decisions on time	✕	✕	✔
14.	Risk response is triggered by indicators status automatically in accordance with risk appetite, tolerance and universe	✕	✕	✔
15.	Responding risk according to risk evaluation	Ⓟ	✔	✕
16.	Monitoring risk continuously	✔	✔	✔
17.	Monitoring ISRM process	✔	✔	✔

✔ **:** Fully addressed Ⓟ **:** Partially addressed ✕ **:** Not addressed

In table-10 all three ISRM models are compared. According to the comparison of ISO/IEC 27000 and NIST 800 series with proposed KRI implemented ISRM model, each of them uses the same metrics and collect them as needed, does not use sample metrics, depends on authorized CISO, and monitors risks and ISRM system continuously (Function no: 1, 4, 5, 11, 16 and 17). All security-related information is in the scope of ISO/IEC 27005 standard, NIST 800 series standards and proposed KRI implemented ISRM model but not in the scope of ISO/IEC 27001 standard. As stated before, correlating and analyzing all security-related information is hardly possible because, resources (time, money, human resources) are scarce. For that, pursuing only key information and metrics are more applicable than to struggle with all information. The proposed KRI implemented ISRM model has those functions where ISO/IEC and NIST series have not (Function no: 2, 3 and 6).

Risk mitigation continuously needs resources, but do we have to mitigate all the risks we have discovered? The proposed KRI implemented ISRM model helps to monitor risks via KRIs and CISOs can decide to execute mitigation processes by establishing the Risk Appetite, Risk Tolerance, and Risk Universe. ISO/IEC 27000 and NIST 800 series advice to list all risks and after analyzing and evaluating risks can be mitigated according to the Risk Management Budget (Function no: 7, 8, 9, 10 and 15). Besides the budget, responding on time is another cost-saving function mentioned in the proposed KRI implemented ISRM model. KRIs trigger responds just on time of risk exposure but both ISO/IEC 27000 and NIST 800 series does not have such a mechanism (Function no: 12, 13 and 14).

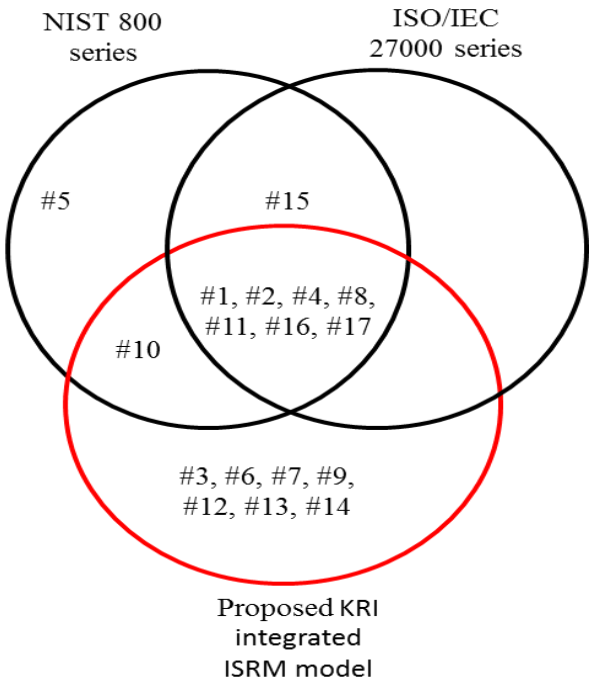


Figure 16: Function distribution Venn diagram

As can be seen from the figure-16, the proposed KRI implemented ISRM model includes 15 functions in which 7 of them not included by the other models. Only the function no:5 is included by NIST 800 series and function no:15 included both by NIST 800 series and ISO/IEC 27000 series ISRM models. Consequently, function distribution shows that KRI implemented ISRM model helps to save risk mitigation budget, facilitates risk monitoring and communicating with superior management by responding to the risks which only started to exposure.

CHAPTER 9

THE SURVEY

9.1. The Problem Statement

ISRM standards like ISO 27000 and NIST 800 series include risk assessment and risk mitigation methods. But these standards do not deal with the resources allocated and senior managements' concern. In order to avoid this concern, KRI based risk monitoring can help to decrease the required resources significantly and increase the risk monitoring effectiveness. KRIs are metrics to monitor changes in the level of risk to take action. They are capable of showing that the organization is subject to or has a high probability of being subject to a risk that exceeds the defined risk appetite. They are related to a specific risk and show changes in the likelihood or consequence of the risk occurring.

9.2. Purpose

The purpose of this study is to get and analyze subject matter experts' opinions about the benefits of implementing KRI into current ISRM models.

9.3. The Research Methodology

A survey was conducted to collect data from subject matter experts. After the survey was developed, it was validated by 10 different subject matter experts with an academic background to see that it complies with the problem statement and is enough to collect the right data. The interview method was used during this validation study. After the 10^{th} interview, it was seen that there were no significant changes suggested any more. 19 questions were asked in the survey and all answers were collected according to the Likert five-point agreement scale (strongly agree, agree, undecided, disagree, strongly disagree). Then the survey in the APPENDIX

F was published during one-month period and more than 450 people or groups were invited to fill in. The people invited in the sample were from software companies, government employee and academic groups from universities. Invitations were made via e-mail and participants were informed that all answers and knowledge would be kept secret and used only for academic study. There were 78 people filled in the survey. At the end of the survey, data was uploaded to SPSS (statistical package for social sciences) for further statistical analyses.

9.4. Hypotheses

This study attempts to examine the following hypotheses based on the study problem and its purpose:

H1: The use of KRI in the implementation of existing ISRM standards enables more efficient use of resources, identification, and detection of risk exposures and facilitates communication related to cybersecurity between the technical team and top management.

H1.1: Institutions' sources are usually not enough for mitigating all risks detected during implementing ISRM standards.

H1.2: When KRI is applied to ISRM standards, resources are used more efficiently because by the help of KRI only the risks to be realized are mitigated.

H1.3: There is a lack of communication between the cybersecurity team and the senior management of the organization about eliminating the risks related to information security.

H1.4: The effective design of KRIs and their harmonization with the big picture provide a stronger connection with the company's board of directors and senior management. Because this provides a non-technical perspective of the program and facilitates the control.

9.5. The Limits of the Study

This study was conducted with subject matter experts and academics working in the field of cybersecurity. However, since the number of experts and academicians working in this field are unknown, the number of samples could not be established and t-test could not be performed to validate the hypotheses.

9.6. Population and Sample

The ISRM standards studied are the best frameworks available worldwide. It could not be found in the literature research that how many people in the world apply these standards, in which countries they were compulsory and whether the countries had their own standards. In this context, the number of study population could not be learned. Therefore, the number of samples could not be revealed. However, 450 cybersecurity experts and academic groups, most of them domestic, were asked to participate in the survey. According to the answers given by 78 people, the results obtained from the collected data were interpreted by percentage majority calculation.

9.7. Analysis and Findings

9.7.1. The Reliability Analysis

Table 11: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,870	,883	19

The Reliability Analysis output showed that Cronbach's alpha is 0,87 which indicates a high level of internal consistency for the 5-point Likert scale (table-11). According to the calculated Cronbach’s alpha, the survey results were 87% reliable.

9.7.2. Demographic Data

Some details about the participants are given below in the charts.

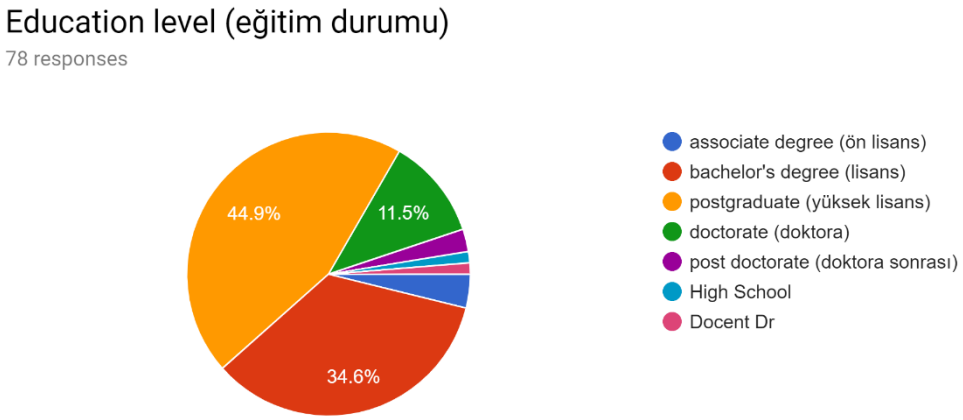


Figure 17: Education Level of Participants

74 people out of 78 have a bachelor's degree and above. The majority of the education level was postgraduate. It followed by the bachelor's degree. It could be said that most of the responders have a high academic degree (figure-17).

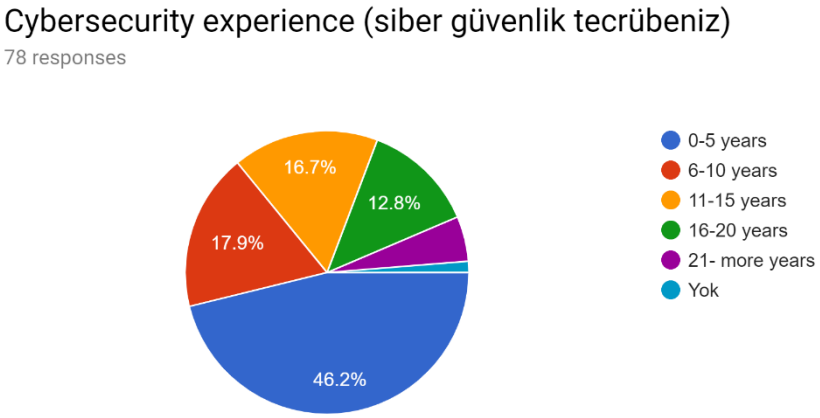


Figure 18: Cybersecurity Experience of Participants

It can be seen from the chart depicted in figure-18 that the cybersecurity experience of the responders is enough to get satisfactory results. Only 1 out of 78

responders does not have any experience. 36 of them have 0 to 5 years' experience, 14 of them have 6-10 years' experience, 13 of them have 11 to 15 years' experience 10 of them have 16 to 20 years' experience and 4 of them have 21 years' experience and more.

9.7.3. Analysis of Answers

There were 19 questions asked to participants and all answers were collected according to the Likert five-point agreement scale (strongly agree, agree, undecided, disagree, strongly disagree).

Table 12: Answer distribution

Total answers	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
1482	42,1%	34,3%	13,4%	6,4%	3,8%

Participants gave total of 1482 answers. The detailed distribution of answers according to the questions can be found in APPENDIX H. Those answers were distributed as seen in table-12:

According to the total results, 1132 answers (76,4%) strongly agreed and agreed with the idea that KRI based risk monitoring can help a significant decrease in the required resources and increase the risk monitoring effectiveness. On the other hand, 152 answers (10,2%) strongly disagreed and disagreed with the idea where 198 could not decide. The frequency and percentage table of each answer for every question can be found in APPENDIX I.

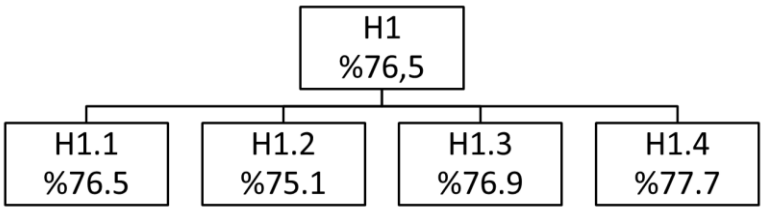


Figure 19: Percentage of "Strongly Agree" and "Agree" Answers

With regards to the hypothesis, it was confirmed that Hypothesis-1, Hypothesis-1.1, Hypothesis-1.2, Hypothesis-1.3 and Hypothesis-1.4 validated by experts with the percentage of 75% or higher (figure-19).

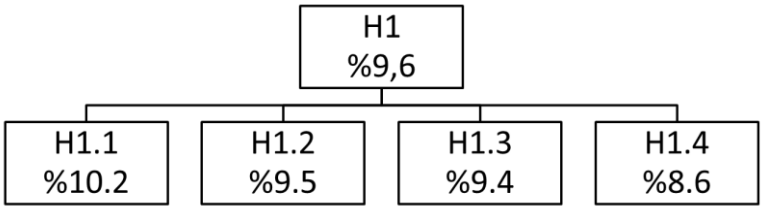


Figure 20: Percentage of "Strongly Disagree" and "Disagree" Answers

According to the results, only few of experts disagree about the benefits of implementing KRI into the ISRM standards (figure-20).

The results show that the majority of experts agreed with the idea of new KRI based ISRM model. The detailed explanation of validation is elaborated below.

Validation of Hypothesis-1

In the APPENDIX J it can be seen that all questions were attached to a related hypothesis.

Table 13: Answers related Hypothesis-1

Total answers	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
1014	40,1%	36,4%	13,9%	6,3%	3,3%

According to this table, questions 7-19 were related to Hypothesis-1 and 1014 answers were collected. 776 answers (76,5%) strongly agreed and agreed with the Hypothesis-1, where 97 (9,6%) did not (table-13).

Validation of Hypothesis-1.1

Questions 1-8, 12 and 14-17 were related to Hypothesis-1.1 and 1014 answers were collected.

Table 14: Answers related Hypothesis-1.1

Total answers	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
1014	41.9%	34,6%	13,3%	6,3%	3,9%

776 answers (76, 5%) strongly agreed and agreed with the Hypothesis-2, where 104 (10,2%) did not (table-14).

Validation of Hypothesis-1.2

Questions 7, 8, 12, 15 and 16 were related to Hypothesis-1.2 and 390 answers were collected.

Table 15: Answers related Hypothesis-1.2

Total answers	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
390	35,4%	39,7%	15,4%	6,7%	2,8%

293 answers (75,1%) strongly agreed and agreed with the Hypothesis-1.2, where 37 (9,5%) did not (table-15).

Validation of Hypothesis-1.3

Questions 12, 14, 15, 17, 18 and 19 were related to Hypothesis-1.3 and 468 answers were collected.

Table 16: Answers related Hypothesis-1.3

Total answers	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
468	39,7%	37,2%	13,7%	6,2%	3.2%

360 answers (76,9%) strongly agreed and agreed with the Hypothesis-1.3, where 44 (9,4%) did not (table-16).

Validation of Hypothesis-1.4

Questions 12-15 and 17-19 were related to Hypothesis-1.4 and 546 answers were collected.

Table 17: Answers related Hypothesis-1.4

Total answers	**Strongly agree**	**Agree**	**Undecided**	**Disagree**	**Strongly disagree**
546	39,6%	38,1%	13,7%	5,9%	2,7%

424 answers (77,7%) strongly agreed and agreed with the Hypothesis-1.4, where 47 (8,6%) did not (table-17).

CHAPTER 10

CASE STUDY

10.1. The Aim of the Study

In Chapter 9, the majority of the experts agreed upon the idea of implementing KRI into ISRM standards. This survey was the first validation step and, in this step, the idea of the thesis is validated. The target of the second step of validation was to prove that KRI could be implemented to the real IT system which had certified ISRM standard. Therefore, I agreed and worked with a company to study implementing KRI into the company's ISMS.

The case study performed with a Software Company. The Company had valid ISO 9001, ISO/IEC 27001, CMMI 5 certificate and NATO Facility Clearance Certificate at the level of 'NATO SECRET'. For security reasons, the Company's name is excluded from the study. All study was conducted together with the Company's CISO and permissions of senior management.

Initially, KRI and its benefits were explained to CISO. Because the Company had ISO/IEC 27001 certificate, I implemented KRI methodology into ISO/IEC 27005 ISRM process. As seen in APPENDIX D, KRI sub-processes were inserted under related processes. Then the Risk Universe, Risk Strategy, Risk Mitigation methods, and Risk Monitoring methods of the Company were investigated. It was clear that the Company had strict rules for IT security. After evaluation, the 3 risks mentioned below were analyzed. A systematical approach for KRI implementation was applied to the Company's ISRM system with the results of the analysis.

10.2. Developing Key Indicator Criteria

Key Indicator Criteria were developed according to the Company's strategy. These criteria can be used as a template because they define standard criteria of good indicators.

Table 18: Criteria List

Criteria no	Criteria
Criteria_1	A key indicator should be relevant to what is being monitored
Criteria_2	A key indicator should be measured at a high level of precision and repetition
Criteria_3	A key indicator should provide sufficient information to understand the exposure levels that the indicator relates to
Criteria_4	A key indicator should be easy to verify
Criteria_5	A key indicator should be simple and relatively cost-effective
Criteria_6	A key indicator should be easy to interpret, understand and monitor

KRIs were designed within these criteria framework. 6 criteria were developed (table-18) and these criteria were considered sufficient to develop KRIs.

10.3. Risk Evaluation

Since the Company had a risk list within the ISO/IEC 27001 certification studies, I only implemented the third dimension for the evaluation process. ISO/IEC 27001 standard uses likelihood and impact dimensions. During this process, the Company's risks were evaluated with KRI eligibility. In addition to the Prioritized Risk List, Key Risk List is developed.

10.4. Defining Key Indicators (attribute)

In the next step, KRIs were identified and their characteristics were specified.

Table 19: Attribute List

Attribute no	Attribute
Attribute_1	Indicators should provide relevant information about the risk exposure
Attribute_2	Indicators should be measured accurately and regularly. Suggested formats are numbers, values, percentages, or ratios. Non-quantitative indicators are subjective and can be misinterpreted
Attribute_3	Selected indicators should predict the changes in the risk profile to take preventive measures
Attribute_4	The data required to calculate the indicators should be available and obtainable. Also, these indications should be appropriate and easily interpretable

At the end of this process, 4 attributes shown in table-19 were developed.

10.5. Assessed Risk List

In the fourth stage, 3 risks were selected from the Company's Risk Universe. The Company's Risk Universe included risks which were previously assessed risks as specified in ISO/IEC 27001 standard.

Table 20: Assessed Risk List

Risk no	Risk
Risk_1	Cyber-attack (virus, Trojan, penetration, breach)
Risk_2	Unauthorized access to system or data
Risk_3	Update version control

The selected risks (table-20) were the same as Key Risk List.

10.6. Selection of Key Risk Indicators

The above-mentioned criteria related to these risks were created with the help of cybersecurity checklists and the Company's CISO.

Table 21: RISK-1 KRI List

KRI no	KRI
R_1/KRI_1	Number of assets not listed in the inventory
R_1/KRI_2	Number of unknown privileged accounts
R_1/KRI_3	Percentage of excessive end-user privileges
R_1/KRI_4	Number of new vulnerabilities
R_1/KRI_5	Percentage of unknown non-human credential activity
R_1/KRI_6	Time period of continuous vulnerability assessment and remediation with automated software
R_1/KRI_7	Time period of continuous data recovery
R_1/KRI_8	Average of the missing person in security awareness education

Table 22: RISK-2 KRI list

KRI no	KRI
R_2/KRI_1	Number of Active Directory changes
R_2/KRI_2	Number of embedded credential discovery
R_2/KRI_3	Percentage of passwords incompatible with security best practices
R_2/KRI_4	Period of updating black-list (malicious IP addresses) and white-list (trusted sites)
R_2/KRI_5	Percentage of invalidated log settings
R_2/KRI_6	Percentage of anomaly traffic flow

Table 23: RISK-3 KRI List

KRI no	KRI
R_3/KRI_1	Number of uncertified applications
R_3/KRI_2	Number of new updates
R_3/KRI_3	Percentage of unsupported application
R_3/KRI_4	Percentage of not updated malware defense applications

A total of 18 KRIs were produced, 8 for the first risk (table-21), 6 for the second risk (table-22) and 4 for the third risk (table-23).

Table 24: Characteristics of Good Key-Indicators

-	**Relevance**
-	**Measurable**
-	**Predictive**
-	**Easy to Monitor**
-	**Auditable**

While selecting these 18 KRIs, it was ensured that they comply with the characteristics of good key-indicators shown in table-24:

After developing the 18 KRIs they were evaluated according to the KRI criteria. APPENDIX E shows that all KRIs were convenient with the all criteria.

10.7. Identify Thresholds

In the next step, thresholds were defined for which levels of alarms would be selected depending on the risk appetite of the KRIs.

Table 25: Definitions of Alarm Levels

Alarm level	Definition
Green Alarm	The risk is within the risk appetite. No any precautions needed but continuous monitoring should continue.
Yellow Alarm	The risk is within the risk appetite but there are strong indicators shows that risk will possibly happen. Preventive precautions should be put in use.
Red Alarm	The risk is out of the risk appetite and tolerance levels. Risk is happening now. All dedicated resources and planned precautions must be put in use immediately.

Table-25 shows that each alarm level was assigned with color by creating a three-level alarm system. Accordingly, the green, yellow and red alarm levels were defined as alarms generated by the monitored KRIs.

10.8. Monitor Metric Changes (Continuous Monitoring of KRIs)

Changes in KRIs were monitored according to the threshold limits. During implementation, only the green warning is received. If yellow or red alert was received, the cybersecurity software was ready to respond according to the approved security plan.

Table 26: Thresholds of First Risk's KRIs

KRI no	KRI	Thresholds		
R_1/KRI_1	Number of assets not listed in inventory	< 2	<2-5 >	> 5
R_1/KRI_2	Number of unknown privileged accounts	< 1	< 1-3 >	> 3
R_1/KRI_3	Percentage of excessive end user privileges	< 2%	<2-4%>	>4%
R_1/KRI_4	Number of new vulnerabilities	< 5	< 5-15 >	> 15
R_1/KRI_5	Percentage of unknown non-human credential activity	<1%	<1-3%>	>3%
R_1/KRI_6	Time period of continuous vulnerability assessment and	< 2 days	< 2-5 days >	> 5 days

	remediation with automated software			
R_1/KRI_7	Time period of continuous data recovery	< 1 days	< 1-3 days >	> 3 days
R_1/KRI_8	Average of missing person in security awareness education	<10%	<10-20%>	>20%

Table 27: Thresholds of Second Risk's KRIs

KRI no	KRI	Thresholds		
R_2/KRI_1	Number of Active Directory changes	< 5	< 5-10 >	> 10
R_2/KRI_2	Number of embedded credential discovery	< 1	< 1-3 >	> 5
R_2/KRI_3	Percentage of passwords incompatible with security best practices	<2%	<2-3%>	>3%
R_2/KRI_4	Period of updating black-list (malicious IP addresses) and white-list (trusted sites)	< 2 days	< 2-5 days >	> 5 days
R_2/KRI_5	Percentage of invalidated log settings	<1%	<1-3%>	>3%
R_2/KRI_6	Percentage of anomaly traffic flow	<1%	<1-2%>	>2%

Table 28: Thresholds of Third Risk's KRIs

KRI no	KRI	Thresholds		
R_3/KRI_1	Number of uncertified applications	< 2	< 2-3 >	> 3
R_3/KRI_2	Number of new updates	< 5	< 5-10 >	> 10
R_3/KRI_3	Percentage of unsupported application	<1%	<1-2%>	>2%
R_3/KRI_4	Percentage of not updated malware defense applications	<1%	<1-2%>	>2%

The thresholds in the table-26, table-27 and table-28 are particularly calculated for the Company's real risks.

10.9. Deciding & Reporting

The alarms generated according to the monitored thresholds automatically reacted with the help of cybersecurity software as indicated in the security plan. When there were update alarms regarding the applications used, CISO implemented it after consultation with the relevant software experts.

10.10. Risk Response

The risks reported in the previous step were being mitigated automatically with the help of cybersecurity software. According to the security plan Treat or Avoid type responses were implemented for this kind of risks. In the case of application updates, the Accept was applied as a response.

Table 29: Response Types

Response type	Definition
Treat	Implement the security measures specified in the security plan. The exposure level must be above the Risk Appetite and Risk Tolerance levels. (red alarm)
Avoid	If the risk cannot be treated and KRIs alarms still above the limits of Risk Appetite and Risk Tolerance then perform the necessary practices for the removal of risk from Risk Universe. (red alarm)
Transfer	If the risk is neither mitigated nor avoided and KRIs alarms still above the limits of Risk Appetite and Risk Tolerance then transferred it to the third parties according to the security plan. (yellow alarm, red alarm)
Accept	Evaluate the residual risk then accept it.

As mentioned earlier, the company uses commercial cybersecurity software to monitor the specified 3 risks. The initial cost of the cybersecurity software is 8.000 USD and the annual license cost is 3.400 USD. The company's CISO reported that it requires additional 1-person manpower to perform the same functions. This manpower costs 24.000 USD per year. Since KRI application is implemented with cybersecurity software, it has been determined that no organizational changes were needed. Following the interview, it was stated that it was possible to keep track of the KRIs of these 3 risks and to follow responses automatically with the purchased cybersecurity software. They also added that the software made it easier to follow the application updates, and with the help of this they could control the impact of updates for the software they coded.

Consequently, although Company's risk monitoring and mitigation method were automated by the help of cybersecurity software, risk monitoring and mitigation methods transferred into to the KRI approach and the risk monitoring was facilitated. By this method, the Company saved near 20.000 USD every year. In addition, KRIs tables above helped senior management to understand the risks and mitigation methods more profound. The map of Company's risk-KRI network is shown in APPENDIX K. The Company accepted the case study document in their library and CISO decided to start implementing the KRI methodology for improvement of ISO/IEC 27001 processes.

CHAPTER 11

SUMMARY, CONCLUSION AND FUTURE WORK

11.1. Summary and Conclusion

Cybercrime is insidious threat and grows every day. Companies, organizations, and nations are allocating a significant amount of budget for providing cybersecurity. Institutions need unlimited resources for cybersecurity because every day a new threat and risk arise. It is certain that the most efficient way to use cybersecurity resources is through risk management. However, because integrated cybersecurity management with risk management will attempt to take precautions against all detected risks, it will not be true to tell that resources are used effectively.

To protect IT systems, the ISRM standards like ISO 27000, NIST 800 series and COBIT 5 frameworks are used as best practices. These standards use various and many metrics to monitor the ISMS. However, large amounts of money, time and human resources are needed to detect, measure and interpret all. Moreover, these standards do not deal with the resources allocated and senior managements' concern. To avoid these concerns, KRI based risk monitoring can help a significant decrease in the required resources and increase the risk monitoring effectiveness.

In this study, we presented a model to make risk monitoring function more effective by using KRIs and to enhance risk management chapters of the international standards which considered as best practices to achieve safe IT Risk Management. By means of this model, risks that are about to be realized are detected and the resources allocated under the risk mitigation will be spent on time and avoid unnecessary resource allocation for the risks that will not be realized. In

addition, risk management and monitoring procedures will be communicated more clearly with senior management.

The model is presented to make risk monitoring function more effective by using KRIs in order to enhance risk management chapters of the international standards which considered as best practices to achieve safe IT management. By means of this model, risks that are about to be realized are detected and the resources allocated under the risk mitigation will be spent on time and avoid unnecessary resource allocation for the risks that will not be realized. In addition, risk management and monitoring procedures will be communicated more clearly with senior management. Top management's confidence in the technical team will also increase due to the use of resources only mitigating actual risks.

In literature and standards researches there was no academic research found about KRI usage with ISRM, except in COBIT 5 for Risk framework it is found that, although KRI subject is mentioned, the framework is based on scenario-based risk prevention methodology.

During literature researches, it was found that, according to the report of Fourv Systems, the model proposed improving the risk management and monitoring in the context of using KRI can be implemented easily ISO/IEC 27000 and NIST 800 series standards or other ISRM standards and frameworks [7].

KRIs are not a holistic solution for risk management but, they are an important tool within risk management and are used to enhance the monitoring and mitigation of risks and facilitate risk reporting [26].

To justify the study first a survey was conducted to analyze subject matter experts’ opinions about new KRI based ISRM model that can figure out costs and benefits, address stakeholders' concerns. There were 19 questions asked to participants and all answers were collected according to the Likert five-point agreement scale. 78 participants gave a total of 1482 answers. The reliability analysis of the survey was calculated as 87% which is enough for the survey’s

validation. According to the total results, 1132 answers (76,4%) strongly agreed and agreed with the idea that KRI based risk monitoring can help to decrease the required resources significantly and increase the risk monitoring effectiveness. On the other hand, 152 answers (10,25%) strongly disagreed and disagreed with the idea where 198 could not decide. The results show that the majority of experts agreed with the idea of new KRI based ISRM model.

With regards to the hypothesis, it was confirmed that Hypothesis-1, Hypothesis-1.1, Hypothesis-1.2 and Hypothesis-1.3 validated by experts with the percentage of 75% or higher. As for Hypothesis-1.4, while 59.34% of answers was given as strongly agree and agree, 8.6% of answers were disagree and strongly disagree.

The hypothesis of this study proved that the majority of cybersecurity experts agree with the hypothesis that to use implementation model of KRI in the existing ISRM standards enables more efficient use of resources, identification, and detection of risk exposures and facilitates communication related to cybersecurity between the technical team and top management.

Then a case study was conducted with a software company. At the end of the study, a systematical approach of KRI implementation into the Company's ISRM was successfully achieved. Although the Company could monitor some of their risks with the help of a commercial software, implementation of KRI made monitoring function more systematically and made it easy to communicate the status of monitored risks to senior management. The Company accepted the case study documents in their library and CISO decided to start implementing the KRI methodology for improvement of ISO/IEC 27001 processes.

The case study justifies that by using KRI, resources can be used efficiently, the risk monitoring process can be developed and risk management subject can become comprehensible by the senior management.

As a result; literature researches, survey of hypothesis, and the case study proved that by implementing the suggested model of KRI into common ISRM standards, resources can be used efficiently, the risk monitoring process can be developed and risk management subject can become comprehensible by the senior management.

11.2. Future Work

With this study, it has been proved that the implementation of KRI to ISRM standards provides benefit for risk monitoring, reducing costs and facilitating communication with senior management. As the continuation of this study, it will be useful to study the necessary changes in the organizational structure of the institutions which will implement the KRI and to study or develop the software that can perform the KRI management.

The organizations implementing the ISRM framework or standards should take into account the organizational structure and apply the necessary organizational changes when they want to implement the KRI structure. Each organization has a culture of its own and KRI implementation is an application that will affect the risk cultures of organizations. For this reason, organizations that want to implement KRI to the ISRM structure should adapt their organizational culture to the KRI concept. I believe that it would be beneficial to conduct a study on the harmonization of the risk culture with the KRI implementation.

Although the KRI follows the realization metrics of the risks, the implementation of these processes through software will increase the KRI efficiency. As I have seen in the case study, the follow-up of the KRI tracking with the help of commercial software makes the process more efficient.

In addition, a common Indicator Library for all risks can be created with another software. In this library, both risks and indicators can be created, developed, matured, monitored and alarm alerts can be generated. Indicators have a life cycle. The indicators formed from the metrics followed by the organization are

monitored and developed within the life cycle. As a result of the experiences, the values, importance, connections, and requirements of the indicators are evaluated again and again. By the help of this evaluation, the necessary adjustments are made in the indicator alarm values, their severity ratings are evaluated, the indicator is needed and the correctness of the connections are examined.

The indicators values will not always be the same. Any changes in the company's IT inventory, changes in the qualitative and quantitative characteristics of human resources, changes in the organizational structure of the company, and changes in the company's business case will affect the indicators. I think that coding a basic library software will contribute to the continuous updating and evaluation of the KRIs.

Since KRI is a practice that may involve changes at any time, it is inevitable that the indicators will change based on the risks that are continuously monitored after the KRI is applied to ISRM. Any experience experienced after the implementation of KRI should be analyzed and changes related to KRI processes should be included in the relevant processes. When the mentioned development processes are supported by Artificial Intelligence, the automation of KRI monitoring function will be realized. In this context, in addition to coding a library, the KRI application can be combined with Deep Machine Learning to create a cyber-immune system of IT systems.

REFERENCES

[1] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, 1st ed. 2007.

[2] D. Antonucci, “Monitoring and Review Using Key Risk Indicators (KRIs),” in *The cyber risk handbook : creating and measuring effective cybersecurity capabilities*, 2017, pp. 159–170.

[3] Center for Strategic and International Studies, “Net Losses: Estimating the Global Cost of Cybercrime,” 2014.

[4] N. M. Radziwill and M. C. Benton, “Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management,” *Softw. Qual. Prof.*, vol. 19, no. 4, pp. 25–43, 2017.

[5] R. Bojanc and B. Jerman-Blažič, “An economic modelling approach to information security risk management,” *Int. J. Inf. Manage.*, vol. 28, no. 5, pp. 413–422, 2008.

[6] S. Bosworth, M. E. Kabay, and E. Whyne, *COMPUTER SECURITY HANDBOOK*, 6th ed. John Wiley & Sons, Inc., Hoboken, New Jersey., 2014.

[7] Fourv Systems, “Objective, Real-Time Cyber Key Risk Indicators Using Existing System and Security Sensor Data to Identify and Quantify Client Security Operations Performance,” 2015.

[8] ISO/IEC 27000:, “ISO/IEC 27000:2016(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary,” *ISO.org [Online]*, vol. 4th Editio, p. 42, 2016.

[9] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, “Cybersecurity risk assessment for SCADA and DCS networks,” *ISA Trans.*, vol. 46, no. 4, pp. 583–594, 2007.

[10] P. Oman, E. Schweitzer, and J. Roberts, “Safeguarding IEDs, substations,

and SCADA systems against electronic intrusions," in *2001 Western Power Delivery Automation Conference*, 2001, no. April 2001, pp. 1–18.

[11] "IBM X-Force Threat Intelligence Index 2017," 2017.

[12] B. Karabacak, "Bilgi Güvenliği Risk Analizi (BiGRA) Yöntemi," GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ, 2003.

[13] R. Richardson, "CSI 15th Annual Computer Crime and Security Survey," 2010.

[14] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model," *J. Inf. Secur.*, vol. 06, no. 01, pp. 24–30, 2015.

[15] R. Böhme, "Security Metrics and Security Investment Models."

[16] M. Brecht, T. Nowey, and R. Böhme, "A Closer Look at Information Security Costs," *Econ. Inf. Secur. Priv.*, pp. 3–24, 2013.

[17] ISO/IEC, "ISO/IEC 27005: 2011," *Information technology--Security techniques--Information security risk management. ISO*. 2011.

[18] E. Şahinaslan, R. Kandemir, and A. Kantürk, "Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme."

[19] S. Morgan, "20th Global Information Security Survey 2017–2018," 2017.

[20] H. Takçı, T. Akyüz, A. Uğur, R. Karabağ, F. Ö. Aktaş, and İ. Soğukpınar, "Bilgi Güvenliği Yönetiminde Risk Değerlendirmesi İçin Bir Model," *Türkiye Bilişim Vakfı Bilgi. Bilim. ve Mühendiliği Derg.*, pp. 47–52, 2010.

[21] S. Y. K. Mo, P. a Beling, and K. G. Crowther, "Quantitative assessment of cybersecurity risk using bayesian network-based model," *2009 Syst. Inf. Eng. Des. Symp.*, pp. 183–187, 2009.

[22] “What is indicator? definition and meaning - BusinessDictionary.com.” [Online]. Available: http://www.businessdictionary.com/definition/indicator.html. [Accessed: 11-Sep-2018].

[23] ISO/IEC, “ISO/IEC 27004: Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation, Ed2,” *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*. 2016.

[24] A. Rodriguez, “The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities Monitoring and review Using Key risk Indicators (KrIs) KrI DeSIgn for Cyber rISK ManageMent,” in *The Cyber Risk Handbook*, 2017, pp. 159–170.

[25] ISACA, “The Risk IT Framework,” 2009.

[26] K. Strachnyi, “Operational Risk: Key Risk Indicators (KRIs) | Workiva,” 2015. [Online]. Available: https://www.workiva.com/blog/operational-risk-key-risk-indicators-kris. [Accessed: 07-Sep-2018].

[27] The Institute of Operational Risk, “Institute of Operational Risk Operational Risk Sound Practice Guidance Key Risk Indicators,” 2010.

[28] P. Matruglio and B. Tymmons, “Key Risk Indicators,” 2014.

[29] A. Pleshakova, “Key Risk Indicators, Explained: Part Two - Nehemiah Security.” [Online]. Available: https://nehemiahsecurity.com/blog/key-risk-indicators-explained-part-two/. [Accessed: 02-Feb-2019].

[30] Australian Finance Department, “Understanding and Developing Key Risk Indicators,” 2016.

[31] H. Mouatassim and A. Ibenrissoul, “Proposal for an Implementation Methodology of Key Risk Indicators System: Case of Investment Management Process in Moroccan Asset Management Company,” *J. Financ. Risk Manag.*, vol. 4, pp. 187–205, 2015.

[32] A. & M. Sheldon, “Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission,” in *2009 42nd Hawaii International Conference on System Sciences*, 2009, no. HICSS ’09, pp. 1–10.

[33] NIST, “Guide For Conducting Risk Assessments,” *NIST Special Publication 800-30 Rev.1*, no. September. U.S. Department of Commerce, Gaithersburg, p. 95, 2012.

[34] G. Locke and P. D. Gallagher, “NIST SP 800-39: Managing information security risk: organization, mission, and information system view,” *NIST Special Publication*. pp. 800–39, 2011.

[35] Ross, Ronald S, Johnson, and La, “NIST Special Publication 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems,” p. 102, 2010.

[36] J. Davies, M. Finlay, T. McLenaghen, and D. Wilson, “Key Risk Indicators – Their Role in Operational Risk Management and Measurement,” *AMA Approaches to Oper. Risk*, pp. 1–32, 2006.

[37] A. Pleshakova, “Key Risk Indicators, Explained: Part One - Nehemiah Security.” [Online]. Available: https://nehemiahsecurity.com/key-risk-indicators-explained-part-one/. [Accessed: 12-Jan-2018].

APPENDICES

APPENDIX A: COMPARISON OF RECOMMENDED MODEL WITH ISO/IEC 27000 SERIES FRAMEWORKS

	FUNCTION	ISO/IEC 27000 Series	Proposed model
01.	Using metrics established by the organization	✔	✔
02.	Collecting, correlating and analyzing ALL security related information	Ⓟ	✔
03.	Collecting, correlating and analyzing KEY security related information	✕	✔
04.	Collecting and analyzing the data regularly and as often as needed	✔	✔
05.	Using sample metrics or data	✕	✕
06.	Collecting and analyzing the KEY metrics continuously	✕	✔
07.	Establishing RISK APPETITE	✕	✔
08.	Acting according to the RISK TOLERANCE (risk acceptance criteria)	Ⓟ	✔
09.	Establishing RISK UNIVERSE	✕	✔
10.	Defining, selecting and monitoring risk indicators/factors	✕	✔
11.	Authorizing CISO to determine whether to conduct risk response in accordance with organizations risk tolerance	✔	✔
12.	Responding according to the exposure of the risk	✕	✔
13.	Having risk response decisions on time	✕	✔
14.	Risk response is triggered by indicators status automatically in accordance with risk appetite, tolerance and universe	✕	✔
15.	Responding risk according to risk evaluation	✔	✕
16.	Monitoring risk continuously	✔	✔
17.	Monitoring ISRM process	✔	✔

✔ **:** Fully addressed Ⓟ **:** Partially addressed ✕ **:** Not addressed

APPENDIX B: COMPARISON OF RECOMMENDED MODEL WITH NIST 800 SERIES FRAMEWORKS

	FUNCTION	NIST 800 Series	Proposed Model
01.	Using metrics established by the organization	✔	✔
02.	Collecting, correlating and analyzing ALL security related information	✔	✔
03.	Collecting, correlating and analyzing KEY security related information	✕	✔
04.	Collecting and analyzing the data regularly and as often as needed	✔	✔
05.	Using sample metrics or data	Ⓟ	✕
06.	Collecting and analyzing the KEY metrics continuously	✕	✔
07.	Establishing RISK APPETITE	✕	✔
08.	Acting according to the RISK TOLERANCE (risk acceptance criteria)	✔	✔
09.	Establishing RISK UNIVERSE	✕	✔
10.	Defining, selecting and monitoring risk indicators/factors	✕	✔
11.	Authorizing CISO to determine whether to conduct risk response in accordance with organizations risk tolerance	✔	✔
12.	Responding according to the exposure of the risk	✕	✔
13.	Having risk response decisions on time	✕	✔
14.	Risk response is triggered by indicators status automatically in accordance with risk appetite, tolerance and universe	✕	✔
15.	Responding risk according to risk evaluation	Ⓟ	✕
16.	Monitoring risk continuously	✔	✔
17.	Monitoring ISRM process	✔	✔

✔ **:** Fully addressed Ⓟ **:** Partially addressed ✕ **:** Not addressed

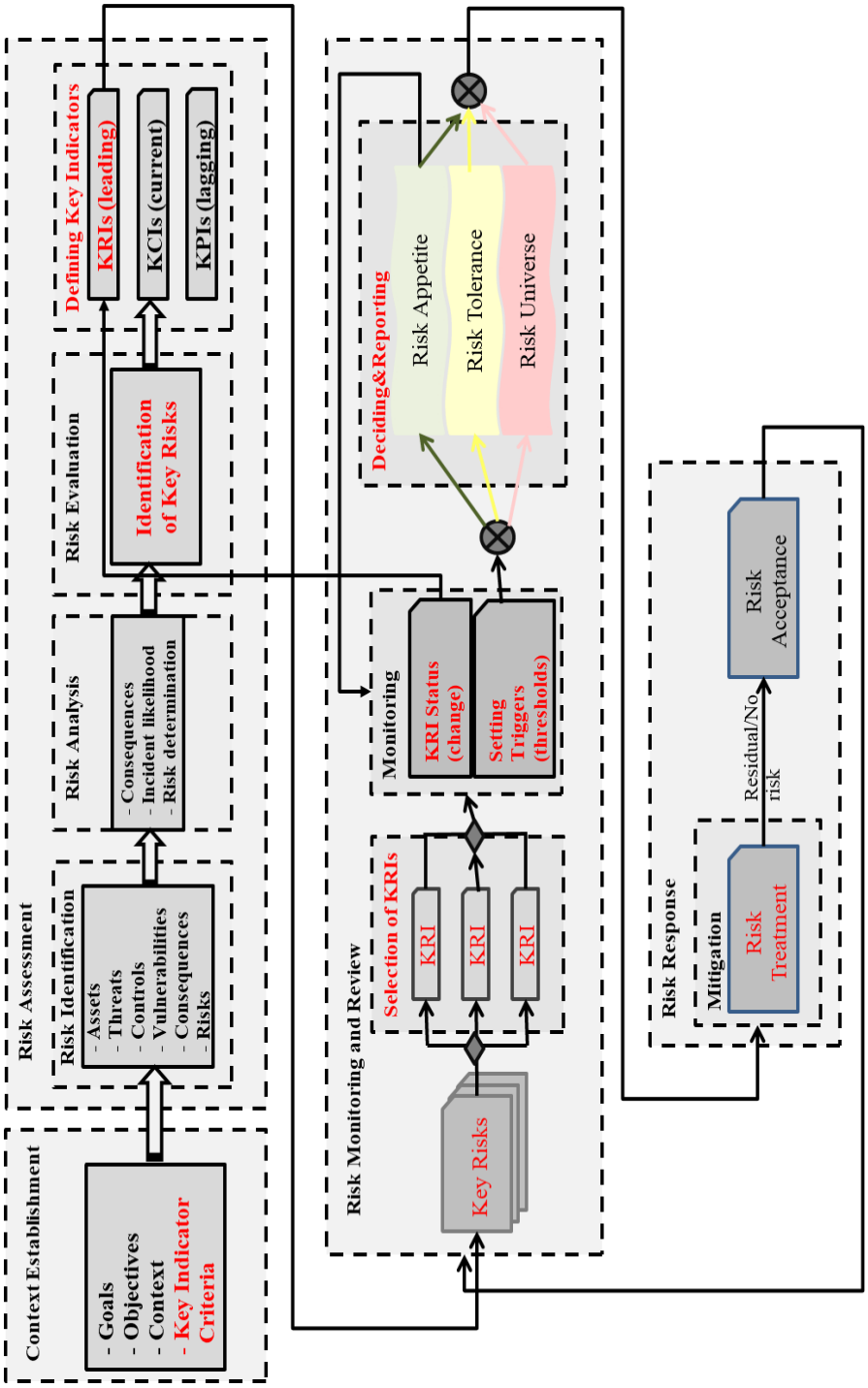
APPENDIX C: COMPARISON OF PROPOSED MODEL WITH ALL RELATED FRAMEWORKS

	FUNCTION	NIST 800-37	NIST 800-137	NIST 800-39	NIST 800-30	ISO/ IEC 27001	ISO/ IEC 27005	Proposed model
01.	Using metrics established by the organization	Ⓟ	✔	Ⓟ	✔	✔	✔	✔
02.	Collecting, correlating and analyzing ALL security related information	✔	✔	✔	✔	✕	✔	✔
03.	Collecting, correlating and analyzing KEY security related information	✕	✕	✕	✕	✕	✕	✔
04.	Collect and analyze the data regularly and as often as needed	✔	✔	✔	✔	✔	✔	✔
05.	Using sample metrics or data	✕	✔	✔	✕	✕	✕	✕
06.	Continuously collect and analyze the KEY metrics	✕	✕	✕	✕	✕	✕	✔
07.	Establish RİSK APPETITE	✕	✕	✕	✕	✕	✕	✔
08.	Act according to the RISK TOLERANCE (risk acceptance criteria)	✔	✔	✔	✕	Ⓟ	Ⓟ	✔
09.	Establish RISK UNIVERSE	✕	✕	✕	✕	✕	✕	✔
10.	Define, select and monitor risk indicators/factors	✕	✕	✕	✔	✕	✕	✔
11.	Authorizing CISO* to determine whether to conduct risk response in accordance with organizations risk tolerance	✔	✔	✔	N/A	✔	✔	✔
12.	Respond according to the exposure of the risk	✕	✕	✕	N/A	✕	✕	✔
13.	Timely risk response decisions	✕	✕	✕	N/A	✕	✕	✔

14.	**Risk response is triggered by indicators status automatically in accordance with risk appetite, tolerance and universe**	✗	✗	✗	**N/A**	✗	✗	✔
15.	Responding risk according to risk evaluation	✗	N/A	✔	N/A	✔	✔	✗
16.	Monitoring risk continuously	✔	Ⓟ	✔	✔	Ⓟ	✔	✔
17.	Monitoring ISRM process	✔	✔	✔	✔	✔	✔	✔

✔ **:** Fully addressed Ⓟ **:** Partially addressed ✗ **:** Not addressed

APPENDIX D: ISO/IEC 27005 ISRM PROCESS AFTER KRI IMPLEMENTATION



APPENDIX E: KRI CONFORMITY TABLE

	Criteria 1	Criteria 2	Criteria 3	Criteria 4	Criteria 5	Criteria 6	Attribute 1	Attribute 2	Attribute 3	Attribute 4	Relevance	Measurable	Predictive	Easy to Monitor	Auditable
R_1/KRI_1	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_1/KRI_2	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_1/KRI_3	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_1/KRI_4	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_1/KRI_5	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_1/KRI_6	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_1/KRI_7	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_1/KRI_8	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_2/KRI_1	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_2/KRI_2	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_2/KRI_3	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_2/KRI_4	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_2/KRI_5	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_2/KRI_6	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_3/KRI_1	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_3/KRI_2	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_3/KRI_3	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
R_3/KRI_4	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

APPENDIX F: SURVEY FOR THE BENEFITS OF USING KEY RISK INDICATORS FOR MONITORING CYBERSECURITY RISKS

The Information Systems Risk Management (ISRM) standards like ISO 27000 and NIST 800 series include risk assessment and risk mitigation methods. But these standards don't interest with the resources allocated and senior managements' concern. For avoiding this concern, Key Risk Indicator (KRI) based risk monitoring can help a significant decrease in the required resources and increase the risk monitoring effectiveness. KRIs are metrics to monitor changes in the level of risk to take action. They are capable of showing that the organization is subject to or has a high probability of being subject to a risk that exceeds the defined risk appetite. They are related to a specific risk and show changes in the likelihood or consequence of the risk occurring.

In this survey, a new KRI based ISRM model that can figure out costs and benefits, address stakeholders' concerns will be evaluated.

ISO 27000 ve NIST 800 serisi gibi Bilgi Sistemleri Risk Yönetimi (ISRM) standartları risk değerlendirmesi ve risk azaltma yöntemlerini içermektedir. Ancak bu standartlar, ayrılan kaynak miktarına ve üst düzey yönetimin endişelerini kapsamamaktadır. Bu endişeden kaçınmak için, Anahtar Risk Göstergesi (KRI) bazlı risk izleme metodu, gerekli kaynaklarda önemli bir azalmaya ve risk izleme etkinliğini artırmaya yardımcı olabilir. KRI'ler, risk seviyesindeki değişiklikleri izlemek için kullanılan ölçümlerdir. Kuruluşun tanımlanmış risk iştahını aşan bir riske maruz kalma olasılığına sahip olduğunu gösterme yeteneğine sahiptirler. Belirli bir risk ile ilgilidir ve gereçekleşmekte olan risk ile ilgili değişiklikler gösterir.

Bu ankette, maliyet ve faydaları azaltabilecek, paydaşların endişelerini giderebilecek yeni bir KRI tabanlı ISRM modeli değerlendirilecektir.

SURVEY FOR THE BENEFITS OF USING KEY RISK INDICATORS FOR MONITORING CYBER SECURITY RISKS
SİBER GÜVENLİK RİSKLERİNİN TAKİBİNDE KRI KULLANIMININ FAYDALARI

Questions below will be asked to cybersecurity specialists and answers will be evaluated in Likert five-point agreement scale. (Strongly disagree, Disagree, Undecided, Agree, Strongly agree)

Aşağıdaki sorular siber güvenlik uzmanlarına sorulacak ve cevaplar Likert beş aşamalı anlaşma ölçeğinde değerlendirilecektir. (Kesinlikle katılmıyorum, katılmıyorum, kararsız, katılıyorum, kesinlikle katılıyorum)
QUESTIONS/SORULAR:

1. According to the most common ISRM Standards like ISO/IEC 27005 and NIST 800-37, it is necessary for IT systems to carry out a risk analysis for the vulnerabilities and the threats and to take proper precautions to eliminate the risks.

Information Security Officers implementing the most common ISRM Standards usually decide to take precautions against ALL detected risks.

ISO / IEC 27005 ve NIST 800-37 gibi en yaygın ISRM Standartlarına göre, BT sistemlerinin güvenlik açıkları ve tehditler için risk analizi yapması ve riskleri ortadan kaldırmak için uygun önlemleri alması gerekir.

En yaygın ISRM Standartlarını uygulayan Bilgi Güvenliği Görevlileri genellikle tespit edilen TÜM risklere karşı önlem almaya karar verir.

2. Depending on the IT system size, cybersecurity precautions and controls cannot cover all the weaknesses of the information system as well as prevent the threats entirely.

BT sisteminin boyutuna bağlı olarak, siber güvenlik önlemleri ve kontrolleri, bilgi sisteminin tüm zayıf yönlerini kapsayamadığı gibi tehditleri de tamamen önleyemez.

3. It is impossible to create a defensive structure for all of the cyber threats.

Tüm siber tehditler için savunma yapısı oluşturmak imkansızdır.

4. To exclude risks usually needs resources.

Riskleri azaltmak için genellikle kaynak gerekir.

5. The most efficient way to use resources is through risk management.

Kaynakları kullanmanın en etkili yolu risk yönetimidir.

6. Since dozens of new risks occur every day, monitoring and mitigating all risks will be either impossible or need a lot of resources.

Her gün düzinelerce yeni risk oluştuğundan, tüm risklerin izlenmesi ve azaltılması ya imkansızdır ya da çok fazla kaynağa ihtiyaç duymaktadır.

7. If the risks about to happen could be determined, the resources allocated under the risk mitigation could be spent on time.

Eğer gerçekleşmekte olan riskler belirlenebilirse, risk azaltma kapsamında tahsis edilen kaynaklar zamanında harcanabilir.

8. If the risks about to happen could be determined, the organization could avoid unnecessary resource allocation for the risks that will not be happened.

Eğer gerçekleşmekte olan riskler belirlenebilirse, organizasyon gerçekleşmeyecek riskler için gereksiz kaynak tahsisinden kaçınabilecektir.

9. Security efforts should be utilized on time and in place.

Güvenlik çabaları zamanında ve yerinde kullanılmalıdır.

10. It is more feasible to collect, correlate and analyze KEY security-related information instead of ALL security-related information.

Güvenlikle ilgili TÜM bilgiler yerine güvenlikle ilgili ÖNEMLI bilgileri toplamak, ilişkilendirmek ve analiz etmek daha uygundur.

11. The ISRM standards such as ISO/IEC 27005 and NIST 800 assess risks and assert to mitigate all risks if possible.

ISO / IEC 27005 ve NIST 800 gibi ISRM standartları riskleri değerlendirmekte ve mümkünse tüm risklerin azaltılmasını gerekli görmektedir.

12. ISRM should include an appropriate risk assessment and risk mitigation method that can figure out expected cybersecurity costs, address stakeholders' concerns, and compatible with legal requirements.

ISRM, beklenen siber güvenlik maliyetleri azaltabilen ve paydaşların endişelerini giderebilecek uygun bir risk değerlendirmesi ve risk azaltma yöntemi içermelidir.

13. KRIs can be used to enhance the monitoring and mitigation of cyber risks and facilitate cyber risk reporting.

KRI'ler, siber risklerin izlenmesini ve azaltılmasını geliştirmek ve siber risk raporlamasını kolaylaştırmak için kullanılabilir.

14. Mitigation of detected risks require additional investment and resources, so senior managers are sometimes having difficulty deciding on these issues.

Tespit edilen risklerin azaltılması ek yatırım ve kaynak kullanımı gerektirdiğinden, üst düzey yöneticiler bazen bu konularda karar vermekte zorlanmaktadırlar.

15. The ISRM standards like ISO 27000 series and NIST 800 series include risk assessment and risk mitigation methods, but these standards don’t interest with the

resource allocation and senior managements' concern. It is more beneficial to include these points inside the standards mentioned above.

ISO 27000 serisi ve NIST 800 serisi gibi ISRM standartları risk değerlendirme ve risk azaltma yöntemlerini içerir ancak bu standartlar, ayrılan kaynak miktarına ve üst düzey yönetimin endişelerini kapsamamaktadır. Bu hususları anılan standartlara dahil etmek daha faydalıdır.

16. KRI based risk monitoring can help a significant decrease in the required resources and increase risk monitoring effectiveness.

KRI temelli risk izleme, gerekli kaynaklarda önemli bir düşüşe ve risk izleme etkinliğini artırmaya yardımcı olabilir.

17. There are differences in knowledge and priorities between the technical team and the senior managers within the scope of setting up an effective defensive establishment with limited resources. IT personnel think more in the technical dimension while managers think in the context of income-expenditure.

Sınırlı kaynaklarla etkin bir savunma tesisinin kurulması kapsamında, teknik ekip ile üst düzey yöneticiler arasında bilgi ve öncelikler arasında farklılıklar vardır. BT personeli teknik boyutta daha fazla düşünürken, yöneticiler gelir-gider bağlamında düşünürler.

18. Risk management and monitoring procedures can be communicated more clearly to senior management using KRI.

Risk yönetimi ve izleme prosedürleri, KRI kullanarak üst yönetime daha net bir şekilde iletilebilir.

19. Top management's confidence in the technical team will increase if resources are used to mitigate only for actual risks.

Kaynakların sadece gerçek riskleri azaltmak için kullanılması durumunda, üst yönetimin teknik ekibe olan güveni artacaktır.

APPENDIX G: APPROVAL OF METU HUMAN SUBJECTS ETHICS COMMITTEE

UYGULAMALI ETİK ARAŞTIRMA MERKEZİ
APPLIED ETHICS RESEARCH CENTER

ORTA DOĞU TEKNİK ÜNİVERSİTİ
MIDDLE EAST TECHNICAL UNIV

DUMLUPINAR BULVARI 06800
ÇANKAYA ANKARA/TURKEY
T: +90 312 210 22 91
F: +90 312 210 79 59
ueam@metu.edu.tr
www.ueam.metu.edu.tr

Sayı: 28620816 / 227

10 Mayıs 2019

Konu: Değerlendirme Sonucu

Gönderen: ODTÜ İnsan Araştırmaları Etik Kurulu (İAEK)

İlgi: İnsan Araştırmaları Etik Kurulu Başvurusu

Sayın Dr. Ali ARİFOĞLU

Danışmanlığını yaptığınız **Fuat ÖZÇAKMAK'ın "Siber Güvenlik Risklerinin Takibinde KRI Kullanımının Faydalarına İlişkin Anket"** başlıklı araştırması İnsan Araştırmaları Etik Kurulu tarafından uygun görülmüş ve **215-ODTÜ-2019** protokol numarası ile onaylanmıştır.

Saygılarımızla bilgilerinize sunarız.

Prof. Dr. Tülin GENÇÖZ
Başkan

Prof. Dr. Tolga CAN
Üye

Doç.Dr. Pınar KAYGAN
Üye

Dr. Öğr. Üyesi Ali Emre TURGUT
Üye

Dr. Öğr. Üyesi Şerife SEVİNÇ
Üye

Dr. Öğr. Üyesi Müge GÜNDÜZ
Üye

Dr. Öğr. Üyesi Süreyya Özcan KABASAKAL
Üye

APPENDIX H: DISTRIBUTION OF ANSWERS ACCORDING TO THE QUESTIONS

Question no	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
Q1	28,2%	35,9%	17,9%	5,1%	12,8%
Q2	61,5%	23,1%	9,0%	3,8%	2,6%
Q3	48,7%	24,4%	11,5%	10,3%	5,1%
Q4	51,3%	32,1%	10,3%	2,6%	3,8%
Q5	42,3%	38,5%	9,0%	9,0%	1,3%
Q6	46,2%	24,4%	15,4%	9,0%	5,1%
Q7	38,5%	44,9%	11,5%	3,8%	1,3%
Q8	37,2%	30,8%	15,4%	12,8%	3,8%
Q9	75,6%	16,7%	2,6%	2,6%	2,6%
Q10	34,6%	32,1%	11,5%	11,5%	10,3%
Q11	32,1%	33,3%	23,1%	7,7%	3,8%
Q12	48,7%	38,5%	9,0%	3,8%	0,0%
Q13	38,5%	43,6%	14,1%	3,8%	0,0%
Q14	42,3%	35,9%	11,5%	7,7%	2,6%
Q15	25,6%	35,9%	20,5%	10,3%	7,7%
Q16	26,9%	48,7%	20,5%	2,6%	1,3%
Q17	47,4%	37,2%	10,3%	1,3%	3,8%
Q18	35,9%	44,9%	14,1%	3,8%	1,3%
Q19	38,5%	30,8%	16,7%	10,3%	3,8%
TOTAL	42,1%	34,3%	13,4%	6,4%	3,8%

APPENDIX I: THE FREQUENCY AND PERCENTAGE TABLE

According to the most common ISRM Standards like ISO/IEC 27005 and NIST 800-37, it is necessary for IT systems to carry out a risk analysis for the vulnerabilities and the threats and to take proper precautions to eliminate the risks. Information Security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	22	28,2	28,2	28,2
	agree	28	35,9	35,9	64,1
	neither agree nor disagree	14	17,9	17,9	82,1
	disagree	4	5,1	5,1	87,2
	strongly disagree	10	12,8	12,8	100,0
	Total	78	100,0	100,0	

Depending on the IT system size, cybersecurity precautions and controls cannot cover all the weaknesses of the information system as well as prevent the threats entirely.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	48	61,5	61,5	61,5
	agree	18	23,1	23,1	84,6
	neither agree nor disagree	7	9,0	9,0	93,6
	disagree	3	3,8	3,8	97,4
	strongly disagree	2	2,6	2,6	100,0
	Total	78	100,0	100,0	

It is impossible to create a defensive structure for all of the cyber threats.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	39	50,0	50,0	50,0
	agree	19	24,4	24,4	74,4
	neither agree nor disagree	9	11,5	11,5	85,9
	disagree	7	9,0	9,0	94,9
	strongly disagree	4	5,1	5,1	100,0
	Total	78	100,0	100,0	

To exclude risks usually needs resources.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	40	51,3	51,3	51,3
	agree	25	32,1	32,1	83,3
	neither agree nor disagree	8	10,3	10,3	93,6
	disagree	2	2,6	2,6	96,2
	strongly disagree	3	3,8	3,8	100,0
	Total	78	100,0	100,0	

The most efficient way to use resources is through risk management.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	32	41,0	41,0	41,0
	agree	30	38,5	38,5	79,5
	neither agree nor disagree	7	9,0	9,0	88,5
	disagree	8	10,3	10,3	98,7
	strongly disagree	1	1,3	1,3	100,0
	Total	78	100,0	100,0	

Since dozens of new risks occur every day, monitoring and mitigating all risks will be either impossible or need a lot of resources.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	37	47,4	47,4	47,4
	agree	19	24,4	24,4	71,8
	neither agree nor disagree	12	15,4	15,4	87,2
	disagree	6	7,7	7,7	94,9
	strongly disagree	4	5,1	5,1	100,0
	Total	78	100,0	100,0	

If the risks about to happen could be determined, the resources allocated under the risk mitigation could be spent on time.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	31	39,7	39,7	39,7
	agree	34	43,6	43,6	83,3
	neither agree nor disagree	9	11,5	11,5	94,9
	disagree	3	3,8	3,8	98,7
	strongly disagree	1	1,3	1,3	100,0
	Total	78	100,0	100,0	

If the risks about to happen could be determined, the organization could avoid unnecessary resource allocation for the risks that will not be happened.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	29	37,2	37,2	37,2
	agree	24	30,8	30,8	67,9
	neither agree nor disagree	12	15,4	15,4	83,3
	disagree	10	12,8	12,8	96,2
	strongly disagree	3	3,8	3,8	100,0
	Total	78	100,0	100,0	

Security efforts should be utilized on time and in place.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	58	74,4	74,4	74,4
	agree	13	16,7	16,7	91,0
	neither agree nor disagree	2	2,6	2,6	93,6
	disagree	2	2,6	2,6	96,2
	strongly disagree	3	3,8	3,8	100,0
	Total	78	100,0	100,0	

It is more feasible to collect, correlate and analyze KEY security-related information instead of ALL security-related information.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	28	35,9	35,9	35,9
	agree	25	32,1	32,1	67,9
	neither agree nor disagree	9	11,5	11,5	79,5
	disagree	9	11,5	11,5	91,0
	strongly disagree	7	9,0	9,0	100,0
	Total	78	100,0	100,0	

The ISRM standards such as ISO/IEC 27005 and NIST 800 assess risks and assert to mitigate all risks if possible.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	25	32,1	32,1	32,1
	agree	26	33,3	33,3	65,4
	neither agree nor disagree	18	23,1	23,1	88,5
	disagree	6	7,7	7,7	96,2
	strongly disagree	3	3,8	3,8	100,0
	Total	78	100,0	100,0	

ISRM should include an appropriate risk assessment and risk mitigation method that can figure out expected cybersecurity costs, address stakeholders' concerns, and compatible with legal requirements.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	38	48,7	48,7	48,7
	agree	30	38,5	38,5	87,2
	neither agree nor disagree	7	9,0	9,0	96,2
	disagree	3	3,8	3,8	100,0
	Total	78	100,0	100,0	

KRIs can be used to enhance the monitoring and mitigation of cyber risks and facilitate cyber risk reporting.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	30	38,5	38,5	38,5
	agree	34	43,6	43,6	82,1
	neither agree nor disagree	11	14,1	14,1	96,2
	disagree	3	3,8	3,8	100,0
	Total	78	100,0	100,0	

Mitigation of detected risks require additional investment and resources, so senior managers are sometimes having difficulty deciding on these issues.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	33	42,3	42,3	42,3
	agree	28	35,9	35,9	78,2
	neither agree nor disagree	9	11,5	11,5	89,7
	disagree	6	7,7	7,7	97,4
	strongly disagree	2	2,6	2,6	100,0
	Total	78	100,0	100,0	

The ISRM standards like ISO 27000 series and NIST 800 series include risk assessment and risk mitigation methods, but these standards don't interest with the resource allocation and senior managements' concern. It is more beneficial to include these points inside the standards mentioned above.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	20	25,6	25,6	25,6
	agree	28	35,9	35,9	61,5
	neither agree nor disagree	16	20,5	20,5	82,1
	disagree	8	10,3	10,3	92,3
	strongly disagree	6	7,7	7,7	100,0
	Total	78	100,0	100,0	

KRI based risk monitoring can help a significant decrease in the required resources and increase risk monitoring effectiveness.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	21	26,9	26,9	26,9
	agree	38	48,7	48,7	75,6
	neither agree nor disagree	16	20,5	20,5	96,2
	disagree	2	2,6	2,6	98,7
	strongly disagree	1	1,3	1,3	100,0
	Total	78	100,0	100,0	

There are differences in knowledge and priorities between the technical team and the senior managers within the scope of setting up an effective defensive establishment with limited resources. IT personnel think more in the technical dimension while managers think in the context of income-expenditure.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	37	47,4	47,4	47,4
	agree	29	37,2	37,2	84,6
	neither agree nor disagree	8	10,3	10,3	94,9
	disagree	1	1,3	1,3	96,2
	strongly disagree	3	3,8	3,8	100,0
	Total	78	100,0	100,0	

Risk management and monitoring procedures can be communicated more clearly to senior management using KRI.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	28	35,9	35,9	35,9
	agree	35	44,9	44,9	80,8
	neither agree nor disagree	11	14,1	14,1	94,9
	disagree	3	3,8	3,8	98,7
	strongly disagree	1	1,3	1,3	100,0
	Total	78	100,0	100,0	

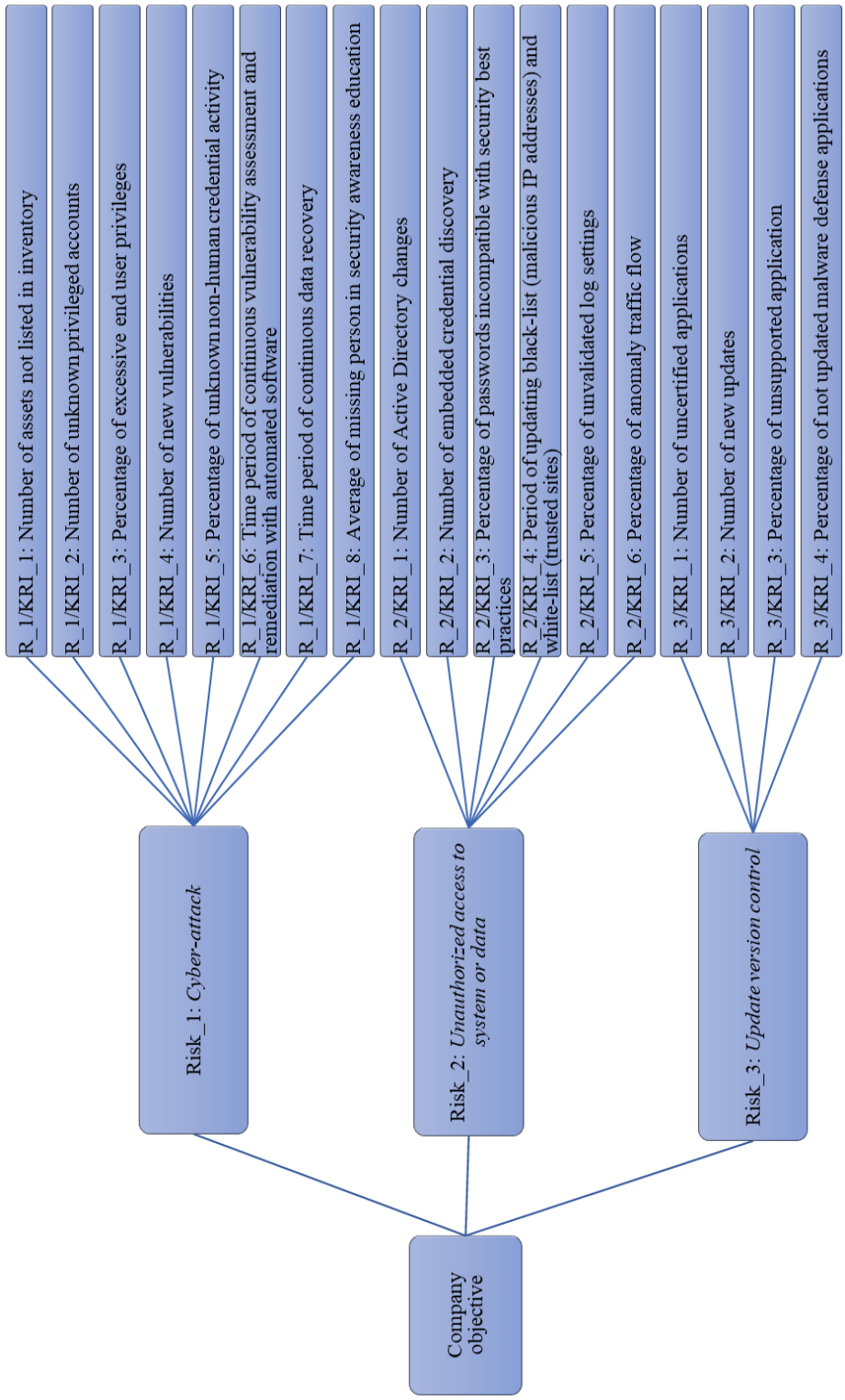
Top management's confidence in the technical team will increase if resources are used to mitigate only for actual risks.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	30	38,5	38,5	38,5
	agree	24	30,8	30,8	69,2
	neither agree nor disagree	13	16,7	16,7	85,9
	disagree	8	10,3	10,3	96,2
	strongly disagree	3	3,8	3,8	100,0
	Total	78	100,0	100,0	

APPENDIX J: QUESTION MATRIX SUPPORTING HYPOTHESIS

	H 1	H 1.1	H 1.2	H 1.3	H 1.4
Q1	-	+	-	-	-
Q2	-	+	-	-	-
Q3	-	+	-	-	-
Q4	-	+	-	-	-
Q5	-	+	-	-	-
Q6	-	+	-	-	-
Q7	+	+	+	-	-
Q8	+	+	+	-	-
Q9	+	-	-	-	-
Q10	+	-	-	-	-
Q11	+	-	-	-	-
Q12	+	+	+	+	+
Q13	+	-	-	-	+
Q14	+	+	-	+	+
Q15	+	+	+	+	+
Q16	+	+	+	-	-
Q17	+	+	-	+	+
Q18	+	-	-	+	+
Q19	+	-	-	+	+

APPENDIX K: THE MAP OF THE COMPANY'S RISK-KRI NETWORK



105

APPENDIX L: LIST OF STANDARDS

- ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary (2016)
- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements (2013)
- ISO/IE 27004 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (2016 ed2)
- ISO/IEC 27005 Information technology — Security techniques — Information security risk management (2011 ed2)
- NIST 800-30 Guide for Conducting Risk Assessments (2012 Rev1)
- NIST 800-39 Managing Information Security Risk (2011)
- NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems (2011 rev1)
- NIST 800-55 Performance Measurement Guide for Information Security (2008 rev1)
- NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (2011)

APPENDIX M: TURKISH SUMMARY/TÜRKÇE ÖZET

Siber suçlar, kriz seviyesine ulaşan sinsi bir tehdittir. McAfee Global Siber Suçlar Maliyeti 2014 raporunda, siber suçlar için küresel ekonomik maliyet tahminlerinin yılda 375 milyar ila 575 milyar dolar arasında olabileceği, ancak doğru bir şekilde ölçülmesinin zor olduğunu belirtilmektedir. Siber suçlar geliştikçe hiçbir sistem güvenli bölgede kalamayacaktır. Her gün yayılan ve güçlenen siber tehditlerin ve aşıları henüz bulunmamaktadır.

Siber saldırılar, bizzat kendi kıyamet günümüzü, kişisel veya sosyal olarak etkilenebileceğimiz olayları yaşamamızı sağlayabilir. Bu saldırılar, finans piyasasını, sağlık kayıtlarını, ulaştırma ağlarını, enerjiyi ve askeri savunma sistemlerini etkileyen bir aralıkta olabilir. Bilgilerin karar vericilere kesin, eksiksiz ve zamanında iletilmesini sağlamak, işletmelerin verimliliğini arttırmaktadır.

Araştırmalar, tüm bu tehditler için bir savunma yapısı oluşturmanın imkânsız olduğunu göstermektedir, çünkü tüm tehditlere karşı bir savunma oluşturmak kendi sistemimizin çalışmasını engelleyecektir. Ayrıca böyle bir savunma tesis etmek tehdidin vereceği zarardan ya da sistemimizin başlangıç maliyetlerinden çok daha fazla kaynak gerektirecektir. Ek olarak, tehditler asla sona ermeyeceğinden, siber savunmayı sürekli güncellemek gerekecektir.

Siber güvenlik kaynaklarını kullanmanın en etkili yolunun risk yönetimi olduğu kesindir. Bununla birlikte, risk yönetimine sahip entegre siber güvenlik yönetimi, tespit edilen tüm risklere karşı önlem almaya çalışacağından, kaynakların etkin bir şekilde kullanıldığını söylemek çok doğru olmayacaktır. Bu durumda, risklerin izlenmesinin önemi artmaktadır. Öte yandan, her gün düzinelerce yeni risk oluştuğundan, tüm risklerin izlenmesi imkânsız olmaktadır.

Birçok kuruluşun siber güvenlik olayları nedeniyle başarısız olduğu bilinmemektedir. Bu belirsizliğin temel nedeni, tehlikeleri cevaplamak için

kullanılan etkili risk politikaları ve biraz da şanstır. Genel olarak, Bilgi Teknolojileri (BT) sistemlerindeki tüm başarısızlıklar siber güvenlikle ilişkili değildir, ancak birçok hizmetin operasyonel etkinliğinin siber olaylardan etkilendiği bilinmektedir. Siber saldırıların etkinliği, gelişme hızı ve karmaşıklığı artarken, BT sistemlerinden yararlanan kuruluşlar aynı hıza uyum göstermeli ve risk stratejilerini yenilemelidir.

Siber güvenlik önlemleri, günümüzde kullanılan risk yönetimi standartlarına uygun şekilde alındığında, önemli miktarda maliyet gerektirmektedir. Bu maliyetler aynı zamanda gerçekleşmemiş riskler için tahakkuk eden maliyetleri de içerir. Bu durumda, kaynaklar asla oluşmayacak risklere harcanır. Burada tespit edilen sorun, BSRY standartlarının Siber Güvenlik personelini tüm risklere karşı önlem almaya zorunlu tutmasıdır. Bu BSRY standartları uygulandığında, tüm riskleri ortadan kaldırmak için kaynaklar harcanmakta, yeni riskler tanımlanır ve izlenirse, ek kaynaklarla tekrar risk azaltma önlemleri alınmaktadır. Bununla birlikte, riskler sınırsızdır, ancak kaynaklar değildir. BSRY standartlarının risk izleme bölümlerinin siber güvenlik maliyetlerini azaltmak için desteklenmesi gerekmektedir. Bu şekilde, sınırlı kaynaklar daha etkin bir şekilde kullanılacak ve gerçekleşmeyen riskler için gereksiz kaynaklar israf edilmeyecektir.

Şirketler, kuruluşlar ve ülkeler siber güvenliklerini sağlamak için önemli miktarda bütçe ayırmaktadırlar. Akademisyenler BT sistemlerinde uygulanan güvenlik kontrollerinin amacını, riski azaltarak tasarruf edilecek kaynakların tespit edilen riskin azaltılması için ayrılan kaynaklara eşitlemek olarak tanımlamaktadırlar.

Siber güvenlik harcamalarının artış hızı, yalnızca BT sistemlerinin kullanımının artmasını değil aynı zamanda tehdidin farkındalığının arttığını da yansıtmaktadır. Bununla birlikte, araştırmalarda, siber güvenliğin gerçekten işe yaramasını sağlamak için yapılan harcamaların karşılaştırmasını gösteren hiçbir bilgi bulunamamıştır.

Kurumlar siber güvenlik için sınırsız kaynaklara ihtiyaç duymaktadır, çünkü her gün yeni tehditler ve riskler ortaya çıkmaktadır. Tüm bu tehdit ve riskleri azaltmak için birçok kaynak gerekebilirken, bu önlemlerin planlandığı gibi uygulanması her zaman mümkün olmayabilir. Bu nedenle, gerçekçi risk yönetimi programlarında amaç sıfır risk olmamalıdır. Riskler tıpkı kaynaklar gibi para ile ölçülmelidir. Bu nedenle, alınacak önlemlere iyi bir değerlendirme ile karar verilmelidir.

Yukarıdaki bahsedilen konular kapsamında bu çalışmanın amacı, ARG'leri kullanarak risk izleme fonksiyonunu daha etkin hale getirecek bir model sunmak ve güvenli BT Risk Yönetimi elde etmek için en iyi uygulamalar olarak kabul edilen uluslararası standartların risk yönetimi faaliyetlerini arttırmak için bir model sunmaktır. Bu model sayesinde, gerçekleşmek üzere olan riskler tespit edilmekte ve risk azaltma kapsamında tahsis edilen kaynaklar zamanında harcanarak ve gerçekleşmeyecek riskler için gereksiz kaynak tahsisinden kaçınılacaktır. Ayrıca, risk yönetimi ve izleme prosedürleri üst yönetimle daha net bir şekilde iletilecektir. Üst yönetimin teknik personele olan güveni de yalnızca gerçek riskleri hafifleten kaynakların kullanılması nedeniyle artacaktır. Bu çalışma kapsamında BSRY standartları kapsamında ARG ile risk izleme sürecinin iyileştirilmesi ve uygulamaları incelenmiştir.

Kaynakların etkin kullanımı temelinde, tüm güvenlik yatırımları kuruluşların amaçları çerçevesinde yapılmalıdır. Bunun için, kuruluşların "bütün" önlemler yerine siber güvenlik konusunda ihtiyaç duydukları "yalnızca gerekli" önlemleri almaları daha uygun olacaktır, buna ek olarak, gerekli önlemleri almak için ihtiyaç duyulan kaynakların etkin kullanımını da desteklenecektir.

Risk yönetimi ve siber güvenliği sağlamak için ISO 27000 serisi, NIST 800 serisi ve COBIT-5 gibi çeşitli standartlar geliştirilmiştir. Bu standartlar sadece en iyi uygulama örneklerini ve çerçevelerini sunmaktadır. Bununla birlikte, tüm BT sistemlerinin farklı risk dünyaları olduğu ve her BT sisteminin temel işlevi değiştiği için ortak bir güvenlik uygulamasını ortaya oymak mümkün değildir. Bu

değişikliklerden ötürü, her BT sisteminin siber güvenlik ve risk değerlendirmesi için kendine uygun yönetim sistemi kurması uygun olacaktır. Burada ifade edilen fikir, risk evreninin zarar veya kayıp olasılığını, BT sisteminin envanter değerini ve üzerinde işlenen bilgilerin değerini, hasar veya kaybın büyüklüğünü belirleyeceğidir.

İşletmeler genellikle kaynaklarının en büyük bölümünü risk azaltma bölümünde yer alan risklere ayırsalar da tüm riskler karşılanamamaktadır. Kaynakların doğru risk için kullanımı çok önemli bir role sahiptir çünkü asla maruz kalmayan riskleri ödemek akıllıca değildir. ARG izlemesi sayesinde gerçekleşmemiş risklerin yıllık bütçesi tasarruf edilebilir. Benzer şekilde, ARG'leri kullanarak riskin gerçekleşme olasılığı daha doğru bir şekilde yeniden hesaplanabilir ve risk azaltma bütçesi buna göre yeniden düzenlenebilir.

Bilişim teknolojilerinin güvenliğinden sorumlu olan üst yönetim, genellikle bu teknolojileri çok tanımayan veya tanımak zorunda olmayan kişilerden oluşmaktadır. Bununla birlikte, bilgi teknolojisinden sorumlu oldukları için, bu sistemlerin güvenliğini doğrudan etkileyen risk analizi sürecinin de farkında olmaları ve hatta dahil olmaları gerekmektedir. Birçok risk analizi yöntemi, organizasyon yöneticilerinin katılımını kolaylaştırmamaktadır. Bunun temel nedeni, süreçte yoğun olarak kullanılan matematiksel ve istatistiksel yöntemlerdir. Sonuç olarak, teknik yöntemlerin kullanılması kurum yöneticilerini tatmin etmeyebilir, çünkü bu araçlar yöneticiler için çok tekniktir ve kuruluş yöneticilerinin risk analizi sürecini anlamaları zordur.

Risk grubundan ne kadar fazla risk hafifletilirse, üst yönetim o kadar iyi hissetmektedir. Ancak, kaynaklar az olduğu için, risklerin bir kısmı BT sistemini tehdit etmeye devam edecektir. ARG tarafından izlenebilecek riskler için ayrılan kaynak israf edilmez ve risk ortaya çıkmaya başlamadıkça tasarruf edilir. Bu şekilde, kaynaklar yalnızca gerçekten gerçekleşmiş risklere harcanabilir.

ISO / IEC 27005 standardına göre, bilgi güvenliği gereklilikleri ile ilgili örgütsel ihtiyaçları belirlemek ve etkin bir BGYS oluşturmak için zorunlu olan BSRY'ye sistematik bir yaklaşım gerekmektedir. Bu yolun kurumun stratejik hedefleri ve kültürü için uygun olması ve özellikle uzun vadeli risk yönetimi ile uyumlu olması gerektiği vurgulanmaktadır. Siber güvenlik ile ilgili tüm çalışmalar, ne zaman ve nerede gerekliyse, zamanında ve yerinde uygun şekilde düzenlenmelidir. Siber güvenlik faaliyetlerinin tamamı BSRY'nin bir parçası olmalıdır. Bu faaliyetler, BGYS'nin hem uygulama hem de işletme aşamalarında ele alınmalıdır. Başka bir deyişle, bir BT sisteminin tehlikelere karşı risk analizi yapması ve ardından risk listesini ortadan kaldırmak için kaynaklar açısından önlem alması gerekir.

Siber savunma kapsamında savunulacak sistemlerin değerlendirilmesi ve risklerin analiz edilmesi mevcut kıt kaynakların etkin kullanımı açısından önemli bir sorun olarak görülmektedir. Bilgi güvenliği sağlama noktasında, kuruluşlar önce siber güvenlik risklerini belirlemeli ve mevcut riskler kuruma göre kabul edilebilir bir düzeye alınmalıdır. Bundan sonra, siber sistem güvenliğinin risk değerlendirmesinden önce kuruluşlar ihtiyaçları doğrultusunda bir risk metodolojisi oluşturmalıdır.

Bu bağlamda, sahip olunan sistemlerin değerini sonuçlandırmak ve savunma çabalarını bu değerlere tahsis etmek için akıllı yaklaşımlar uygulamak kaçınılmaz olacaktır. Sistemlerin değerini belirleyebilmek için, saldırıların sonuçlarını ve rakip veya saldırganın asıl amacını değerlendirmek gerekir.

İzleme ve ölçme, bir bilgi sistemi güvenlik performansını ve BGYS'nin etkinliğini ölçerken yapılması gereken ilk eylemlerdir. Bilgi güvenliği için çok sayıda değerin ölçülmesi söz konusu olduğunda, hangi değerlerin ölçüleceğine karar vermek zordur. Bu konu çok önemlidir, çünkü uygulanabilirliği zor, pahalı ve çok fazla veya yanlış ölçüm yapma olasılığı nedeni ile neredeyse mümkün değildir. Anahtar metrikler büyük miktarlarda veri için kullanılabilir, böylece bu olumsuz yönlerden etkilemeden uygun ölçümler yapılabilir.

Risk yönetimi, BT yöneticilerinin faydalandığı süreçtir. Kuruluşun hedeflerine ulaşması için gerekli kritik sistemleri korumak için kullanılır. Bu sürecin amacı, kuruluşun genel risk toleransına uygun olarak etkileneceği riskleri azaltmaktır. Kuruluşların tüm riskleri ortadan kaldırması beklenmemektedir; bunun yerine, stratejik amaçlarını engellemeyebilecek tolere edilebilir bir risk seviyesi tanımlamaya ve ortaya çıkarmaya çalışırlar. Risk yönetimi süreci, risk analizi, risk değerlendirmesi ve risk izleme alt süreçlerini içerir.

Bilgi güvenliğini sağlama noktasında kuruluşlar, önce belirtilen alt süreçleri kullanarak bilgi güvenliği risklerini belirlemeli ve mevcut risklerin kuruluş tarafından kabul edileceği bir seviyeye geçmelidir. Kurumlar ayrıca bilgi güvenliği risk değerlendirmesi yapmadan önce ihtiyaçları doğrultusunda bir risk metodolojisi oluşturmalıdır.

Risk Göstergesi, bir kuruluşun, işine güvenli bir şekilde devam edebilmesi için risk seviyesindeki değişiklikleri izlemesini sağlayan bir ölçümdür. Risk Göstergeleri, kurumun belirli bir zamanda sahip olduğu operasyonel risk seviyesi hakkında spesifik bilgi sağlar. Bu bilgiyi sağlamak için, Risk Göstergesi maruz kaldığı riski gösteren belirli bir ölçüm ile anlaşılabilir ve açık bir ilişki içinde olmalıdır. Risk Göstergeleri eylem noktalarını vurgular. Ayrıca, gerçekleşecek risklerin öncü göstergeleri olabilir. Bunlar genellikle “ileriye dönük” veya “öncü” göstergelerdir.

Bir gösterge önemli bir ölçüm olarak seçildiyse, "anahtar" olarak adlandırılır. Bu anahtar göstergeler performans, risk ve kontrol süreçleri hakkında bilgi açığa çıkarabilir. Ayrıca, her bir ayrı katmanda kararlar almak için belirli risk sahipleri ve sorumlu bölümler kurulması uygun olmaktadır.

ARG'ler risk yönetimi için kapsamlı bir çözüm olmasa da risk yönetimi bağlamında değerli bir araç olarak kabul edilir. Ayrıca, risklerin izlenmesini ve azaltılmasını artırmak ve risk raporlamasını kolaylaştırmak için kullanılırlar.

Bunlar belirli bir risk ile ilgilidir ve meydana gelebilecek riskin gerçekleşme ihtimalini göstermektedir.

Etkili ARG'lerin oluşturulması, kuruluşun amacını ve hedeflerini açıkça anlamada yatar. Etkili bir ARG ölçüm seti, hedeflerin gerçekleştirilmesini etkileyebilecek veya yeni fırsatların varlığını ortaya çıkarabilecek potansiyel riskler hakkında hayati bilgiler verebilir.

ARG'ler, kuruluşların stratejileri ve hedefleri nedeniyle farklıdır. Bunun için her organizasyon için eşsizdirler. ARG'lerin gelişimi ve seçimi, organizasyonun komplikasyonu ve kapsamı gibi farklı parametrelere dayanmaktadır.

Hedeflerden bir veya daha fazlasını etkileyebilecek çeşitli potansiyel kritik riskler vardır. ARG'lar, riskin maruz kalmasıyla ilgili Bilgi Güvenliği Yönetimi ve Üst Yönetim'e bilgi vermek amacıyla kritik risklerle bağlantılıdır. Bu bilgiler önceden belirlenen eşikler sayesinde bir "alarm" olarak ortaya çıkmaktadır. Alarm ile birlikte Üst Yönetim, şirketin hedeflerine ulaşmak ve stratejisini gerçekleştirmek için risk azaltma planını uygulamaya karar verebilir. Bazı ARG'ler yalnızca bir riske bağlıyken, diğerleri birden fazla riske bağlanabilir.

Bir kuruluşta, risk göstergeleri olarak çalışmak üzere geniş bir metrik grubu geliştirilebilir; ancak, tüm metrik kümelerini araştırmak veya izlemek uygun değildir. Özellikle bu setler önemli miktarda olduğunda, artık kontrol edilemezler. Bu yüzden yapmamız gereken sadece "kilit" göstergeler olan önemli göstergelere odaklanmaktır. ARG'ler diğer göstergelerden farklıdır, çünkü bunlar yüksek düzeyde önemlidir ve yüksek olasılıkla kilit riskleri tahmin eder veya gerçekleştiğini gösterir. Bu husus risk yönetimini ve risk izlemeyi kolaylaştırır.

ARG'lerin riskleri izlemek için kullanılması kuruluşa aşağıdaki avantajları getirebilir:

- "İleriye dönük" veya "öncü" ARG'lerle, proaktif bir eylem sağlamak için erken uyarı ayarlanabilir.

- “Geriye doğru bakıldığında” geçmiş olaylardan öğrenmeye devam edebilirsiniz.

- Risk iştahını ve toleransını izlerken, riskin gerçekleşeceği bir noktada karar verebilir ve riske dayalı kazancı maksimize edebilirsiniz.

- ARG'ler karar vericilerin ve risk yöneticilerinin gerçek zamanlı olarak karar vermeleri ve harekete geçmeleri için kolay ve basit uyarılar verir.

- ARG'ler, organizasyon yönetiminin risklerdeki eğilimleri takip etmesine yardımcı olur. Bu, daha fazla yatırımın gerekli olabileceği veya fırsatların ortaya çıkabileceği alanların belirlenmesine yardımcı olabilir.

Herhangi bir organizasyonda kullanılabilecek standart veya evrensel bir ARG seti hazırlamak mümkün değildir. Bunun nedeni, her riskin aynı olmaması ve kuruluşlar için spesifik etki derecelendirmelerinin farklı olmasıdır. Ayrıca, göstergelerin ölçüm sıklığı da önemli bir faktördür. Daha sık ölçülen göstergelerden daha faydalı veriler elde edilecektir.

ARG gelişimi için yayınlanan uluslararası bir standart veya en iyi uygulama kitabı yoktur, çünkü her bir işletmenin amacına ve hedeflerine yönelik riskler farklılıklar göstermektedir. Araştırmalarda, kurumların çoğunun kendi risk yönetiminde kullanılmak üzere kendi ARG geliştirme prosedürlerini geliştirdikleri görülmektedir. Kimlik Tespiti, Seçimi, Kurulması ve Raporlanması gibi prosedürler kurumların çoğunda aynı olmakla birlikte, Risk Kaynaklarının Tanımlanması, Risk Azaltma Planlaması ve Yanıtlama gibi diğer prosedürler farklı şekilde geliştirilmiştir.

ARG'lerin etkili tasarımı ve kurumların stratejileri ve hedefleri ile uyumları, şirketin yönetim kurulu ve üst yönetimi ile daha güçlü bir bağlantı sağlar. Bu programa teknik olmayan bir bakış açısı sağlar ve kontrolü kolaylaştırır. Verimli ARG tasarımının temel amacı, riskin belirli bir zamanda gerçekleştiğini algılamak

ve tespit etmek için riskle ilgili faaliyetleri izlemek ve riski önlemek veya azaltmak için siber güvenlik planına göre risk azaltma faaliyetlerini uygulamaktır.

ARG, risk toleransı ve risk iştahının dengeli olduğu bir noktada ikaz mekanizması sağlayarak maliyetleri düşürmeye yardımcı olur. Ayrıca bir kuruluşun belirli bir riske ne kadar dayanabileceğini belirler ve risk azaltma işleminin ne zaman ve ne kadar uygulanacağını belirler. ARG ile ana riskin ortaya çıkma olasılığı izlenir. Buradaki amaç, riskin risk iştahının belirlediği seviyeye kadar alınmasını sağlamaktır. Risk iştahı, bilgi sistemlerinin kurulu olduğu şirkete göre değişebilir veya kuruluşun risk çerçevesi dahilinde belirlenebilir. Tüm risklerin ortadan kaldırıldığı sistemlerde, güvenlik politikaları ve uygulamaları sistemin çalışmasını çok zorlaştırmakta ve kullanıcıların birçok güvenlik düzenlemesinden geçmesi beklenmektedir. Bu durumda, kullanıcılar sistemi kullanmak konusunda daha isteksiz olma eğilimindedirler veya güvenlik açıklarını kullanarak işleri kolaylaştırmaya çalışırlar.

Bu Risk Evreninin, özellikle de önemli olanların risklerini takip ettiğimizde, ARG kullanarak istediğimiz zaman risk önleme veya azaltma kararları verebiliriz. Bu noktada yapmamız gereken karar süresini belirlemek için eşikler geliştirmektir.

İyi ARG geliştirmek başka önemli bir konudur. İyi ARG kalitesi için standart olmamasına rağmen, akademisyenler neredeyse aynı özellikleri tanımlamaktadırlar:

- Alaka Düzeyi: Göstergeler, kuruluşun riske maruz kalması hakkında gerekli bilgileri sağlamalıdır;

- Ölçülebilirlik: Göstergeler doğru ve düzenli bir şekilde ölçülmelidir. Önerilen biçimler sayılar, değerler, yüzdeler veya oranlardır. Nicel olmayan göstergeler özneldir ve yanlış yorumlanabilir;

- Tahmin edilebilirlik: Seçilen göstergeler, önleyici tedbirlerin alınması için kuruluşun risk profilindeki değişikliklerin bir tahminini sağlamalıdır;

- İzleme imkânı: Göstergeleri hesaplamak için gerekli veriler mevcut ve uygun fiyatlı olmalıdır. Ayrıca, bu göstergeler ilgili olmalı ve kolayca yorumlanabilir olmalıdır.

Tez kapsamında sadece uluslararası kabul görmüş ve uygulamalı olarak onaylanmış Bilgi Güvenliği Risk Yönetimi Standartları risk metodolojisi olarak değerlendirilmiştir. Bu standartlar, belirtilen standartların sürecini kuran, uygulayan ve belgeleyen kuruluşları onaylamalıdır.

Literatürdeki mevcut kaynaklar kapsamında, araştırmaya dahil edilebilecek standartlar kapsamında bir sivil toplum kuruluşu olan Uluslararası Standardizasyon Örgütü (ISO) tarafından yayınlanan "ISO / IEC 27000 serisi standartları" ve ABD hükümetinin BT sistemlerine uyması gereken NIST 800 serisi BSRY belgeleri uygun standartlar olarak incelenmiştir.

Önerilen BSRY modelinde, Risk İzleme ve Gözden Geçirme süreçlerini geliştirmek için aşağıda belirtilen yeni alt süreçler eklenmiştir:

- Anahtar Gösterge Kriterlerinin Geliştirilmesi,
- Risk değerlendirmesi,
- Anahtar Göstergelerin Belirlenmesi,
- Anahtar Risk Göstergelerinin Seçimi,
- ARG'lerin Sürekli İzlenmesi,
- Karar Verme ve Raporlama,
- Risk azaltma.

Önerilen BSRY modelinde, diğer NIST ve ISO / IEC modellerinin aksine, risk azaltma ve izleme ARG'ler tarafından gerçekleştirilmektedir. Buradaki amaç, henüz gerçekleşmemiş riskler için kaynakların harcanmasını önlemektir. Bu amaca

ulaşmak için, Anahtar Gösterge Kriterleri, İçerik Tanımlaması aşamasında tanımlanmıştır. Daha sonra, Anahtar Gösterge Kriterlerine göre, Risk Değerlendirme Aşamasında tanımlanan Temel Riskler ve ARG'ler öncesi Anahtar Göstergeler geliştirilmiştir.

Önerilen Modelin en önemli kısımlarından biri Risk İzleme ve Gözden Geçirme Sürecidir. Kilit Riskler ve ARG'ler bu süreçte risklerle eşleştirilir ve ARG'lerin izlenmesine başlanır. ARG'ler tarafından kurulacak alarmlara, Risk İştahına ve Risk Toleransı Düzeylerine göre hem Risk Sorumlusuna hem de Üst Yönetim'e durum rapor edilmektedir. Risk Yanıt Sürecinde, Bilgi Güvenliği Sorumlusu gibi ilgili birim tarafından risk muamelesi, kaçınma veya devir işlemi gerçekleştirilir. Kalan Risk kabul edilir ve tekrar üst yönetime rapor edilir. Riskler ortaya çıkmaya başladıktan sonra planlı önlemler alınmaktadır. Bu nedenle, gerçekleşmemiş riskler için ayrılan kaynaklar tasarruf edilir.

ISO / IEC 27000 serisi ve NIST 800 serisi BSRY standartları, önerilen ARG entegreli BSRY modeli ile 17 fonksiyonel alanda karşılaştırılmıştır. Bu alanlar BSRY modellerini daha etkin hale getirmek, bütçeleri korumak, riskleri kolayca izlemek ve bunlara müdahale etmek için geliştirilmiştir.

Yapılan çalışmada ISO / IEC 27001, ISO / IEC 27005, NIST 800-30, NIST 800-37, NIST 800-39 ve NIST 800-137 standartları önerilen ARG entegreli BSRY modeliyle karşılaştırılmıştır.

ISO / IEC 27000 ve NIST 800 serisinin önerilen ARG uygulamalı BSRY modeliyle karşılaştırılmasına göre, tüm modeller aynı ölçümleri kullanır ve gerektiğinde veri toplar, örnek ölçümleri kullanmaz, yetkili Bilgi Güvenliği Sorumlusuna bağlıdır ve riskleri ve BSRY sistemini sürekli izler. Güvenlikle ilgili tüm bilgiler ISO / IEC 27005 standardı, NIST 800 serisi standartları ve önerilen ARG BSRY modeli kapsamındadır, ancak ISO / IEC 27001 standardı kapsamında değildir. Daha önce de belirtildiği gibi, güvenlikle ilgili tüm bilgileri ilişkilendirmek ve analiz etmek pek mümkün değildir, çünkü kaynaklar (zaman,

para, insan kaynakları) azdır. Bunun için sadece kilit bilgilerin ve metriklerin takip edilmesi tüm bilgilerle mücadele etmekten daha uygulanabilir. Önerilen ARG uygulanan BSRY modeli, ISO / IEC ve NIST serilerinin olmadığı fonksiyonlara sahiptir.

Risk azaltma işlemi sürekli olarak kaynaklara ihtiyaç duyar, ancak keşfettiğimiz tüm riskleri azaltmak zorunluluğu nereden kaynaklanmaktadır? Önerilen ARG'nın uygulamalı BSRY modeli, ARG'ler üzerinden risklerin izlenmesine yardımcı olur ve Bilgi Güvenliği Sorumluları Risk İştahı, Risk Toleransı ve Risk Evren'i kurarak azaltma süreçlerini yürütmeye karar verebilir. Tüm risklerin listelenmesi ve risklerin analiz edilmesi ve değerlendirilmesinden sonra ISO / IEC 27000 ve NIST 800 serisi BSRY'ler tüm risklerin azaltılmasını istemektedir. Bütçenin yanı sıra, zamanında yanıt vermek, önerilen ARG uygulamalı BSRY modelinde belirtilen bir diğer maliyet tasarrufu işlevidir. ARG tespit ettiği riske maruz kaldığı anda yanıt verir, ancak hem ISO / IEC 27000 hem de NIST 800 serisi böyle bir mekanizmaya sahip değildir.

Tez konusunun doğruluğunu ölçmek maksadıyla konu uzmanlarından veri toplamak için bir anket yapıldı. Anket geliştirildikten sonra, konuya uyduğunu ve doğru verileri toplamak için yeterli olduğunu görmek için akademik geçmişe sahip 10 farklı konu uzmanı tarafından onaylanmıştır.

Ankette 19 soru soruldu ve tüm cevaplar Likert beş aşamalı anlaşma ölçeğine göre toplandı (kesinlikle katılıyorum, katılıyorum, kararsızım, katılmıyorum, kesinlikle katılmıyorum). Daha sonra anket bir aylık sürede yayınlandı ve 450'den fazla kişi veya grup doldurmaya davet edildi. Örnekte davet edilenler yazılım şirketlerinden, devlet çalışanlarından ve üniversitelerden gelen akademik gruplardandı. Anketi toplamda 78 kişi doldurdu. Anketin sonunda, istatistiksel analizler için veriler SPSS yazılımına yüklendi.

İcar edilen anket çalışması, konu uzmanları ve siber güvenlik alanında çalışan akademisyenler ile gerçekleştirilmiştir. Bununla birlikte, bu alanda çalışan

uzman ve akademisyenlerin sayısı bilinmediğinden, örnek sayısı belirlenememiştir ve hipotezleri doğrulamak için t-testi yapılamamıştır.

İncelenen BSRY standartları dünya çapında mevcut en iyi çerçevelerdir. Literatür araştırmasında dünyadaki kaç kişinin bu standartları uyguladığı, hangi ülkelerde zorunlu olduğu ve ülkelerin kendi standartlarına sahip olup olmadığı tespit edilememiştir. Bu bağlamda, çalışma nüfusunun sayısı öğrenilememiştir. Bu nedenle, örneklerin sayısı hesap edilememiştir. Bununla birlikte, ankete çoğu yurt içinden olmak üzere 450 siber güvenlik uzmanı ve akademik grubun katılması istenmiştir. 78 kişinin verdiği cevaplara göre, toplanan verilerden elde edilen sonuçlar yüzde çoğunluk hesaplaması ile yorumlanmıştır.

Güvenilirlik Analizi çıktısı, Cronbach'ın alfa değerinin 0,87 olduğunu gösterdi ki bu 5 puanlık Likert ölçeği için yüksek bir iç tutarlılık düzeyi olduğunu göstermiştir. Elde edilen toplam sonuçlara göre, uzmanların %76,4'ü ARG temelli risk izlemenin gerekli kaynaklarda önemli bir azalmaya yardımcı olabileceği ve risk izlemenin etkinliğini artıracağı fikrini kabul etti. Öte yandan, %10,2'si ise aynı fikirde değildi.

Anket sonuçlarına göre ortaya konan tüm hipotezler uzmanlar tarafından %75 veya daha yüksek yüzde oranıyla doğrulanmıştır.

Yapılan anket sonuçlarına göre uzmanların çoğu, ARG'yı BSRY standartlarına uygulama fikri üzerinde hemfikirdi. Bu anket ilk doğrulama adımıydı ve bu aşamada tez fikri doğrulanmış oldu. İkinci doğrulama adımının hedefi, ARG'nın BSRY standardını onaylamış olan gerçek IT sistemine uygulanabileceğini kanıtlamaktı. Bu nedenle, ARG'yı şirketin BGYS'sine uygulama konusunda çalışmak için bir şirketle anlaştım ve birlikte çalıştım.

Şirket, "NATO GİZLİ" düzeyinde NATO Tesis İzin Belgesi'ne ve ISO 9001, ISO / IEC 27001, CMMI 5 sertifikasına sahiptir. Güvenlik nedeniyle, Şirket'in adı çalışma dışında bırakılmıştır. Tüm çalışma Şirket'in Bilgi Güvenliği Sorumlusu ve üst yönetimin izinleri ile birlikte yapılmıştır.

İlk olarak, ARG ve faydaları Bilgi Güvenliği Sorumlusuna açıklandı. Şirket ISO / IEC 27001 sertifikasına sahip olduğundan, ARG metodolojisini ISO / IEC 27005 BSRY sürecine uyguladım. Bu kapsamda ARG alt süreçleri ilgili süreçlere eklenmiştir. Daha sonra Şirketin Risk Evreni, Risk Stratejisi, Risk Azaltma yöntemleri ve Risk İzleme yöntemleri incelenmiştir. Şirketin BT güvenliği için katı kurallara sahip olduğu açıktı. Değerlendirmeden sonra, belirlenen 3 risk analiz edildi. Analiz sonuçları ile birlikte Şirket BSRY sistemine ARG uygulaması için sistematik bir yaklaşım uygulanmıştır.

Sonuç olarak, Şirket'in risk izleme ve azaltma yöntemi, firmanın satın aldığı bir siber güvenlik yazılımı sayesinde otomatik olarak uygulansa da ARG uygulaması ile risk izleme ve azaltma yöntemleri kolaylaştırılmış ve sistematik bir hale getirilmiştir. Bu yöntemle her yıl 20.000 ABD doları tasarruf edebilmesi sağlanmıştır. Ek olarak, üst yönetimin riskleri ve azaltma yöntemlerini daha derinlemesine anlamalarına yardımcı olmuştur. Şirket vaka çalışması dokümanlarını kütüphanesine koymayı kabul etti ve Bilgi Güvenliği Sorumlusu, ISO / IEC 27001 süreçlerinin iyileştirilmesi için ARG metodolojisini uygulamaya başlamaya karar verdi.

Bu çalışmada, ARG'leri kullanarak risk izleme fonksiyonunu daha etkili hale getirmek ve güvenli BT Risk Yönetimi elde etmek için en iyi uygulamalar olarak kabul edilen uluslararası standartların risk yönetimi bölümlerini geliştirmek için bir model sunduk. Bu model sayesinde, gerçekleşmek üzere olan riskler tespit edilmekte ve risk azaltma kapsamında tahsis edilen kaynaklar zamanında harcanacak ve gerçekleşmeyecek riskler için gereksiz kaynak tahsisinden kaçınılacaktır. Ayrıca, risk yönetimi ve izleme prosedürleri üst yönetimle daha net bir şekilde iletilecektir.

Model, güvenli BT yönetimi elde etmek için en iyi uygulamalar olarak kabul edilen uluslararası standartların risk yönetimi bölümlerini geliştirmek için ARG'leri kullanarak risk izleme fonksiyonunu daha etkin hale getirmek için sunulmuştur. Bu model sayesinde, gerçekleşmek üzere olan riskler tespit edilmekte ve risk azaltma

kapsamında tahsis edilen kaynaklar zamanında harcanarak ve gerçekleşmeyecek riskler için gereksiz kaynak tahsisinden kaçınılacaktır. Ayrıca, risk yönetimi ve izleme prosedürleri üst yönetimle daha net bir şekilde iletilecektir. Üst yönetimin teknik takıma olan güveni de yalnızca gerçek riskleri hafifleten kaynakların kullanılması nedeniyle artacaktır.

Literatür ve standart araştırmalarında, BSRY ile ARG kullanımı ile ilgili herhangi bir akademik araştırma bulunamamıştır, sadece Risk çerçevesi için COBIT 5 uygulamasında ARG konusundan bahsedilse de uygulamanın senaryo bazlı risk önleme metodolojisine dayandığı bu nedenle ARG entegrasyonu içermediği tespit edilmiştir.

ARG'ler risk yönetimi için bütünsel bir çözüm değildir, ancak risk yönetimi için önemli bir araçtır ve risklerin izlenmesini ve azaltılmasını geliştirmek ve risk raporlamasını kolaylaştırmak için kullanılmaktadır.

Sonuç olarak; literatür araştırmaları, hipotez anketi ve örnek olay çalışması, önerilen ARG modelini ortak BSRY standartlarına uygulayarak kaynakların verimli bir şekilde kullanılabileceğini, risk izleme sürecinin geliştirilebileceğini ve risk yönetimi konusunun üst yönetim tarafından anlaşılabilir hale geldiğini kanıtlanmıştır. Tez kapsamında ortaya konan model literatürde ilk defa tanımlanmıştır.

APPENDIX N: TEZ İZİN FORMU/THESIS PERMISSION FORM

ENSTİTÜ / INSTITUTE

Fen Bilimleri Enstitüsü / Graduate School of Natural and Applied Sciences [ ]

Sosyal Bilimler Enstitüsü / Graduate School of Social Sciences [X]

Uygulamalı Matematik Enstitüsü / Graduate School of Applied Mathematics [ ]

Enformatik Enstitüsü / Graduate School of Informatics [ ]

Deniz Bilimleri Enstitüsü / Graduate School of Marine Sciences [ ]

YAZARIN / AUTHOR

Soyadı / Surname : Özçakmak
Adı / Name : Fuat
Bölümü / Department : Science and Technology Policy Studies

TEZİN ADI / TITLE OF THE THESIS (**İngilizce** / English): Supplementing ISRM Models by KRI Implementation

TEZİN TÜRÜ / DEGREE**:** **Yüksek Lisans** / Master [X] **Doktora** / PhD [ ]

1. **Tezin tamamı dünya çapında erişime açılacaktır. /** Release the entire work immediately for access worldwide. [X]
2. **Tez iki yıl süreyle erişime kapalı olacaktır.** / Secure the entire work for patent and/or proprietary purposes for a period of **two year. *** [ ]
3. **Tez altı ay süreyle erişime kapalı olacaktır.** / Secure the entire work for period of **six months**. ***** [ ]

***** *Enstitü Yönetim Kurulu Kararının basılı kopyası tezle birlikte kütüphaneye teslim edilecektir.*
A copy of the Decision of the Institute Administrative Committee will be delivered to the library together with the printed thesis.

Yazarın imzası / Signature ..... **Tarih** / Date .....