RELATIONSHIP BETWEEN THE PARAMETERS OF INFORMATION SECURITY RISK MANAGEMENT PROCESS

BURAK ÇAKIL

YEDİTEPE UNIVERSITY

January, 2021

RELATIONSHIP BETWEEN THE PARAMETERS OF INFORMATION SECURITY RISK MANAGEMENT PROCESS

BY

BURAK ÇAKIL

MSc THESIS

IN

MANAGEMENT INFORMATION SYSTEMS (MIS)

YEDİTEPE UNIVERSITY

January, 2021

PLAGIARISM

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

Date:

Name/Surname: Burak ÇAKIL

ABSTRACT

Due to recorded incidents of Information technology inclined organizations failing to respond effectively to threat incidents, this thesis guideline the benefits of conducting a comprehensive risk assessment which would aid proficiency in responding to potential threats. The ultimate purpose is primarily to identify, quantify and control the key threats that are destructive to achieving business objectives.

At the same time, this thesis performs a detailed risk assessment for a case study organization. It contains risk assessment steps, how to apply risk mitigation and effectiveness evaluation after risk assessment in risk management and explains relationship between parameters of the information security risk management processes. The five assets are being defined by organization for risk assessment process. Qualitative analysis techniques are being used to determine possible threats and vulnerabilities in case study. This analysis technique provided clearly determining risk each threat and each asset and vulnerability in organization.

As a result of assessment of risk appetite concept, acceptable risks have been defined. It is come out biggest information security risk because of willingly or unwillingly human error as a result of the analysis. All in all, to reduce the impact of risks that is determined as a result of risk assessment has been used efficient control methods that is identified by defense in depth concept.

ÖZET

Günümüzde kayda geçen bilgi teknolojileri olayları nedeniyle, organizasyonlar, kurumlar bu tehdit içeren olaylara karşı etkili bir biçimde yanıt vermekte zorluk çektiler. Bu tez, potansiyel tehditlere yanıt vermede zorlanan organizasyonlara yardımcı olmak için kapsamlı bir risk değerlendirmesi yapmanın faydalarını açıklamaktadır. Asıl amaç, öncelikle iş hedeflerine ulaşmada engel olan temel tehditleri belirlemek, ölçmek ve kontrol altına almaktır.

Aynı zamanda bu tez, bir vaka çalışması organizasyonu için ayrıntılı bir risk analizi gerçekleştirir. Risk değerlendirme adımlarını, risk yönetiminde risk değerlendirme sonrası risk azaltma ve etkinlik değerlendirmesinin nasıl uygulanacağını içerir ve bilgi güvenliği risk yönetimi süreçlerinin parametreleri arasındaki ilişkiyi açıklar. Risk değerlendirme süreci için organizasyon tarafından beş temek varlık tanımlanmaktadır. Vaka çalışmasında olası tehditleri ve güvenlik açıklarını belirlemek için nitel analiz teknikleri kullanılmaktadır. Bu analiz tekniği, her bir tehdidin ve her bir varlığın ve organizasyondaki güvenlik açıklıklarının neler olduğunun belirlenmesini sağlamıştır.

Risk iştahı kavramının değerlendirilmesi sonucunda kabul edilebilir riskler tanımlanmıştır. Yapılan analizler sonucunda isteyerek veya istemeyerek yapılan insan hatası nedeniyle en büyük bilgi güvenliği riski ortaya çıkmaktadır. Sonuç olarak, risk değerlendirmesi sonucunda belirlenen risklerin etkisini azaltmak için derinlemesine savunma kavramı ile belirlenen etkin kontrol yöntemleri kullanılmıştır.

ACKNOWLEDGMENTS

I would first like to thank my thesis advisor Assoc. Prof. Aşkın Demirağ of the Social Sciences Institute at Yeditepe University. The door to Prof. Demirağ office was always open whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this paper to be my own work but steered me in the right the direction whenever he thought I needed it.

Finally, I must express my very profound gratitude to my parents for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

PREFACE

This thesis focus on Information Security Risk Management process with a case study organization and explains relationship between parameters of Information Security Risk Management.

The goal of thesis is explaining step by step the relationship between the parameters of information security risk management process. It will contribute to literature better understanding of information security risk management process and mitigating their risks in terms of information security vulnerabilities.

At the same time, this thesis provides and contribute to literature:

Robust Information Risk Management brings competitive advantage through an increase in trust that will improve the company's reputation. Effective Information Risk Management lowers the chances of a damaging information security incident.

Mastering Risk Management gives us the visibility and confidence to make better business decisions. Information Risk Management can save money through more efficient controls, more effective architectures, and appropriate levels of protection. Information security risk management provides timely identification and mitigation of the cybersecurity risk.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

When any organization's security has been endangered. It is so effortless action to learn cyber security news such as a private server or web site was hacked or a notebook was stolen. All that incidents are so crucial due to confidential or sensitive data may have been lost, modified or broken integrity of data. Advanced communities are attached importance to transmission and easy access of information, encrypted storage and information security. Information is a data that is defined worthy asset and needs to be kept safely against unauthorized access.

Information security is frequently consist of the accountability, availability, integrity and confidentiality (Blakley, McDermott, & Geer, 2002). Protection of information towards unauthorized access attempts can be defined as Confidentiality. To keeping safely information towards unauthorized transfer, destruction or change of sensitive data is being defined as Integrity. To providing secure access for end users particularly throughout cyber-attacks like DOS (denial of service) or DDOS towards information systems is being defined as Availability. Determining responsibilities, following the instructions and tracking the system activities are being named Accountability.

To allocate big part of budget for information security, the organizations generally limit their sources. The budget and sources should be dedicated according to values of sensitive data and assets and likely cyber-threats. In fact, information security is known a problem of risk management (Schneier, 2000). Thinking whole valuable assets or

information is kept secure during cyber-attacks is not sensible (Decker, 2001). The bad guys can achieve everything with limitless sources and decisiveness. Even if organizations think everything is secured. However, there is always probability of accomplish compromise on likely target organization. The organizations must intend to compose information security rules and policy to reduce risks to acceptable risk levels in place of accept whole risks. Organizations should implement periodically information risk analysis on their network to create and update own security policy (Peltier, 2005).

1.1 Background

Risk is a result of in case of probability of harm and occur when harm happens. All process like mitigating risks to acceptable level, evaluating risk and identifying risk applying specific policies and frameworks can be defined as Information risk management (IRM). It is not possible to say we are %100 secure organization network. Because there can always be cyber-threats and vulnerabilities on organization network. The important thing, determining threats, evaluating the possibility of harm for organization, finding reasons of damages and later taking necessary actions to mitigate the risk to acceptable level which organization accept.

Risks is not identified only on network or computer. It can be defined different types. For example, If the organization take over another organization. The action is not just purchasing another organization. At the same time, organization takes over the exist risks in new organization. If the organization intend to growth as financial. That brings to staff and warehousing needs, want more additional reserve and capital to obtain necessary

tools and for increasing marketing share and sales. In that scenario, if this additional burden does not support by sales. That results in for organization decreased profitability.

The organizations should be always prepared against new risks and taken necessary actions on time according to information security. Some reasons of risks are being listed below.

• **Human interaction** Intentional or accidental action or inaction which can hurt productivity
• **Application error** Buffer overflows, input errors and computation errors
• **Equipment malfunction** Peripheral devices and failure of systems
• **Inside and outside attacks** Attacking, cracking and hacking
• **Loss of data** Unintentional or intentional loss of information to unauthorized receivers
• **Physical damage** Natural disasters, power loss, vandalism, water, and fire
• **Misuse of data** Espionage, sharing trade secrets, theft and fraud

Organizations should define likely cyber-threats to assess and calculate possible harm of threats to organization. It is so difficult to calculate quantity of actual risk. However, determining risk level according to their impact will help to organization in terms of quick action to prevent the risks.

Risk management may be divided into the three processes shown in Figure 1 (NIST, 2002; Farahmand, Navathe, Sharp, & Enslow, 2003; Alberts & Dorofee, 2002; Vorster & Labuschagne, 2005). It should be noted that there is not universal agreement on these processes, but most views share the common elements of risk assessment and risk mitigation (Microsoft, 2004; Hoo, 2000). Risk assessment is generally done to understand the system storing and processing the valuable information, vulnerabilities, possible threats, likely impact of those threats, and the risks posed to the system.

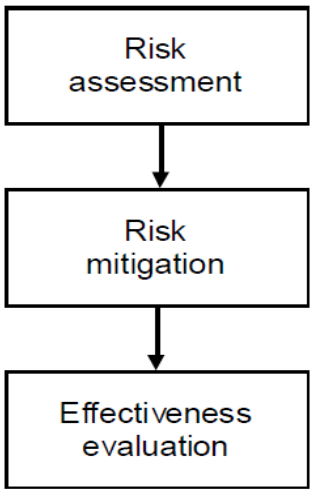

Figure 1 *Steps in risk management.*

Risk assessment would be simply an academic exercise without the process of risk mitigation. Risk mitigation is a strategic plan to prioritize the risks identified in risk assessment and take steps to selectively reduce the highest priority risks under the constraints of an organization's limited resources such as, lack of threat intelligence, auditing and monitoring tools to identify new cyber threats and take an action quickly, lack of budget for personnel training about information security awareness etc.

Third step is effectiveness evaluation. The purpose is to evaluate and confirm that the objectives of risk mitigation have been met. Otherwise, the stages in risk assessment and risk mitigation may have to be updated or altered. In fact, effectiveness evaluation answers to first two transaction to make validation. Besides, the organization network is not constant and changes something forever. To update the risk mitigation strategy by new up to date information there must be applied continuous assessment procedure periodically on organization.

1.2 Purpose

Performing risk evaluation in order to accomplishing business objectives is so critical in terms of determining cyber-threats and vulnerabilities that is prevent organization's future. To decrease risk level from critical to lowest will be used risk assessment's outcome. Besides, this outcome will be used to design necessary risk mitigations plans.

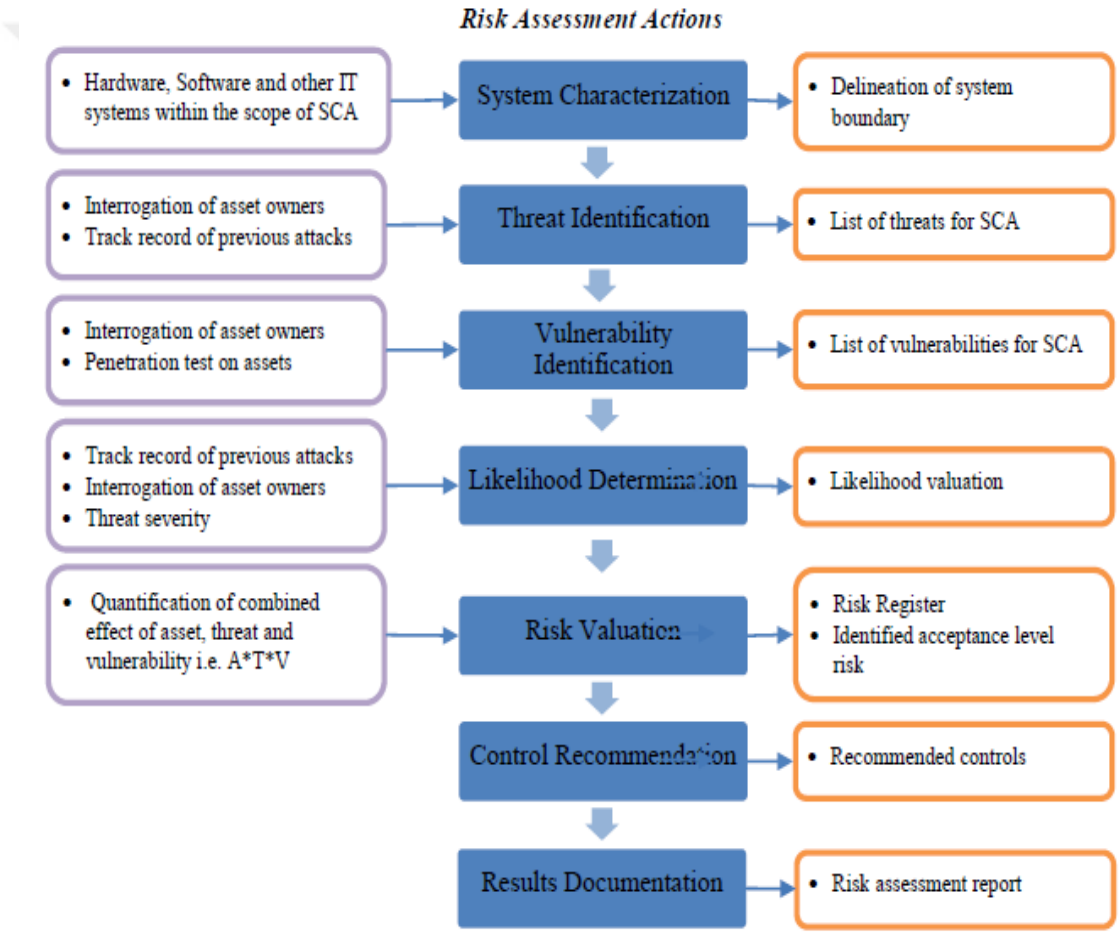

Figure 2 *Risk Assessment Flowchart (G. Stone burner, A. Goguen & A. Feringa;2002)*

Risk assessment process is demonstrated in Figure 2. It explains step by step how to perform risk assessment and determining risks at any organization

1.3 Scope and Assets

In the case study, it has been identified important assets organization's business purposes considering management necessities. Table 1 was used to gather information and determine about organization's assets and asset's values, cyber-threats and vulnerabilities from organization's asset owners. All in all, it is being evaluated probability and effect of the defined cyber-threats on organization with identified model.

Asset Values	Type of effect level of effect	Company embarrassment level	Personal safety implication	Personal privacy infringement	Failure to meet legal obligations	Financial loss (£)	Disruption to activities (£) (time & effort to recover from incident)
1	**Insignificant**	Contained within Work Area at worst	Minor injury to individual	Isolated personal detail revealed	Civil suit resulting in less than £10k damages	Up to 10k	Up to 10k
2	**Minor**	Contained within Company at worst	Minor injury to several people	Isolated personal detail compromised	Civil suit (above £10k). Small fine (up to £1k)	10k to 100k	10k to 100k
3	**Significant**	Local public or Press become aware	Major injury to individual	Several personal details revealed	Large fine (above £10k)	100k to 500k	100k to 500k
4	**Major**	National public or Press become aware	Major injury to several people or death of individual	Several personal details compromised	Custodial sentence imposed	500k to 1000k	500k to 1000k
5	**Acute**	Senior Staff forced to resign or Company fails	Death of several people	All personal details revealed and/or compromised	Multiple civil or criminal suits	Above 1000k	Above 1000k

Table 1 *Asset Values using Impacts of Incidents Matrix*

The five valuable assets of organization were defined sensitive information in kind of electronic data considering data transfer on network after organization management review and approval. Besides, the systems such as physical IT hardware (servers, end user data) that is identified and frequently used by all organization. Other sensitive organization assets defined as the software Revenue Management System(RMS) in order to use to manage business information process and Organization Reputation as intangible assets that

identifies if its business 7 agreements be preserved or terminated in following years and the last one is Human Resource(personnel) that is defined the weakest connection in the information security chain.

2. RISK ASSESSMENT AND ANALYSIS

It is not feasible to understand for specific which cyber-attacks will take place. Risks are depending on what can take place. Therefore, risk based on the probability of a cyber-threats. Besides, if the organization network is preserved against likely threats organization may not be affected to much by possible threats. Additionally, Risk can be defined as a component of the vulnerabilities and influence of the possible threats such as Worms, Viruses, Trojans, Spyware, Riskware, Rootkits etc. Risk evaluation process consist of a figure of stages to know the worth of assets, vulnerabilities, likely cyber-threats, threat probability, and probably effects.

To measure of information's value, the organization must answer some questions such as how much costs of keep secure information, which remediation is necessary to improve, which harm will turn out in case of sensitive information exposed, how much the attacker will pay because of data theft. To protect or keep sensitive information and knowing how much budget should allocate and how long time must spare, is so important thing in terms of take right actions for organization.

Likelihood of the threat to damage organization assets can be defined as a risk. Besides, there is business impact in case of risk occur on organization. Many types of threats such as malware, hacker, users, fire, employee, contractor, attacker and uninvited guest may take benefit various of vulnerabilities on organization and it can be happened

new types of threats on organization valuable assets. The threats that are defined different can be exist in organization network and it's so difficult to define that threats. Besides, that threats can be related by willingly or unwillingly human error or application based. To prevent and explore new threats about application and human error are so hard to identify due to applications have complexities. To defining application codes and issues is so hard for organizations. Besides, it can cause cascading errors and illogical processing in case of that issues occur. Auditing and tracking the organization network in terms of activities help to determining mistakes that is done willingly or unwillingly by human. To monitoring staff errors such as creating weak password, altering data, compromise data integrity, faulty data input on applications, organizations must implement audit periodically on their network and examine.

The organizations have to research and examine of results in terms of risk after determining vulnerabilities and threats. The risks always have possible damages for organizations. That means, the organization can loss their all assets in case of used vulnerabilities by an attacker. The damage can be like modified sensitive data, data theft, data loss, data breach, sharing confidential information, decreasing staff productivity etc. Processes of risk evaluation is demonstrated in Figure 3 as below.

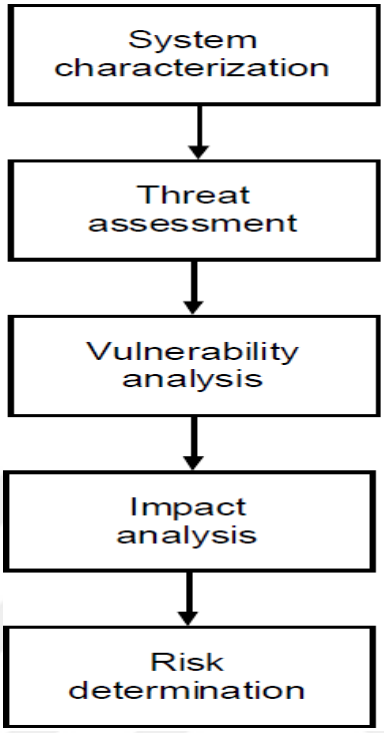

Figure 3 *Steps in risk assessment.*

Organizations should always implement Risk analysis to prevent threats, providing cost-effective security on time, appropriate. Information security may be costly in terms of its complexity. If the organization take precaution too much or insufficient security controls or allocate big part of their budget for information security. That can bring to organization financial burden and this is easy option. Implementing Risk analysis assists to organization to determining and priority of risks and to preserving towards possible threats and how much sources will be able to allocate.

The four basic purposes for a Risk analysis:

• Determine assets and their value to the organization.

• Determine vulnerabilities and threats.

• Calculate the likelihood and business impact of these possible threats.

• Create a financial equalize between the cost of the counterplot and the impact of the threat.

To compare annualize expense of controls with possible cost of damage, Risk analysis uses in order to determine cost-benefit issues for organizations. If annualize expense of damage does not exceed annualize expense of the control, it means organizations do not need to perform control. For example, if the organization is value $50,000. Allocating the budget $100,000 to keep secure of using some control is not correct action.

Understanding and know what we will do first is so crucial thing before start to work in-dept. It means if there is no plan about what organization will do in a project. The project will not make progress properly during process, everybody knows that in organization. Project sizing should be done to know which organization assets and possible threats must be determined before doing risk analysis and assessment. The risk assessments which are done for organizations are generally implemented on staff security, physical security, or information technology security. It is so hard to implement assessment for entire types of security simultaneously.

The person or team that is responsible for organization risk assessment should composed report which contains assets' value list. And then, that list must be presented to

senior management to check and admit. Besides, all these are should be defined as a scope for information risk management (IRM) project. In the beginning of the risk assessment project, management should decide what assets are not significant for organization and which assets does not need to allocation sources or budget during risk assessment process. And then, everybody that is work for the project should clearly understand relationship between business purposes and information security AIC.

Financial restrictions according to organization compliance needs in terms of budget for risk assessment project must be defined and summarized by management. As there has not been done project sizing, lots of projects are resulted without completed because of lack of budget. For this reason, the projects are being generally stopped.

To combining organization business needs with information security purposes should implement risk analysis on organization. If the purposes for business and information security is in harmony each other. Both of them will be accomplish. Besides, it guides to organization about allocation appropriate budget for information security program needs. If the organization knows and learns likely threats that is compromise their valuable assets. It helps to determine necessary action plans for organization related how much budget allocation will be done to keep secure their assets.

If the organization wants to be successful, senior management should encourage to making risk analysis periodically. Later, business objectives and content of the risk analysis should be determined by management. Besides, the management should assign a team that is responsible for risk analysis and then allocate a budget and time. The outputs or results of the risk analysis and assessment must be examined by senior management and determined an action plans according to evidence.

2.1 Positioning Risk Management and Risk Assessment

It seems to be generally accepted by Information Security experts, that Risk Assessment is part of the Risk Management process. After initialization, Risk Management is a recurrent activity that deals with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy. On the contrary, Risk Assessment is executed at discrete time points (e.g. once a year, on demand, etc.) and – until the performance of the next assessment - provides a temporary view of assessed risks and while parameterizing the entire Risk Management process. This view of the relationship of Risk Management to Risk Assessment is depicted in Figure 4 as adopted from OCTAVE.

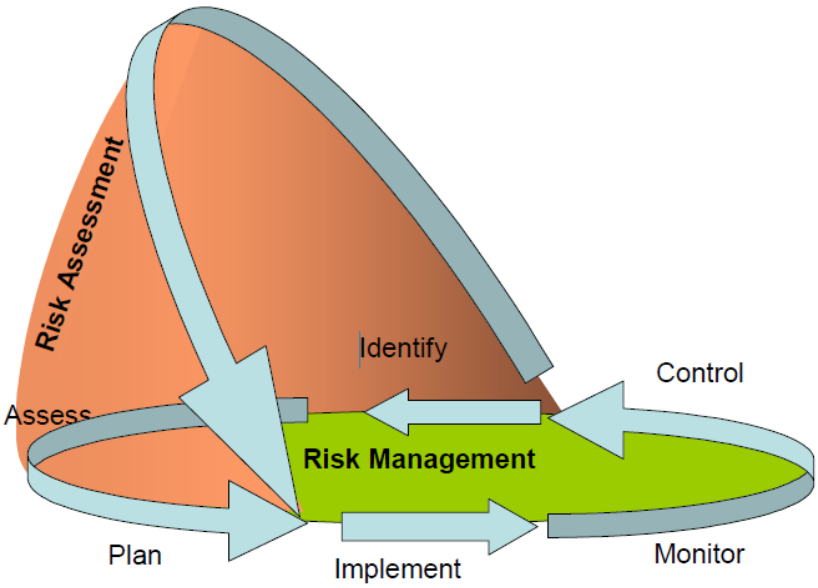

Figure 4 *The relationship between Risk Management and Risk Assessment*

Various standards and good practices exist for the establishment of these processes (e.g. through structuring, adaptation, re-configuration etc.). In practice, organizations tend to generate their own instantiations of these methods, in a form most suitable for a given organizational structure, business area or sector. In doing so, national or international standards (or combination of those) are taken as a basis, whereas existing security mechanisms, policies and/or infrastructure are adapted one-by-one. In this way, new *good practices* for a particular sector are created.

2.2 Identifying Information Assets and Values

An information asset is any information or asset that is valuable to your business and contributes to its ability to operate and its profitability. Typically, you need to look for things like paper or electronic documents, applications, databases, infrastructure, even key people.

The assets may be defined by qualitative and quantitative metrics. However, necessary metrics must be reproduced from organization structure. Organization should take into account how much significant the assets for the organization to identify value of the assets. In this way, organization can calculate real value of the assets. In case of decrease an asset's value, real value of asset must project whole possible costs. For example, if an asset's price $2000 to buy, value of an asset can’t be determined as a purchased price in the risk analysis and assessment process. On the contrary, if the asset has an issue or not working something on it, organization should take into account financial burden of repairing or replacing and cost of data loss to calculate or determine correctly damage for organization.

Below subjects must be paid attention to calculate or determine values of an assets:

• Expense to obtain or enhance the asset

• Expense to preserve and maintain the asset

• Expense of the asset to owners and end users

• Expense of the asset to enemies

• Cost others are willing to pay for the asset

• Expense to replace the asset in case of lost

• Operational and production activities affected in case of the asset is unavailable

• Responsibility subjects in case of the asset is compromised

• Practicability and role of the asset in the organization

Determining which security technologies must be implemented and how much budget must be allocated to prevent attacks to the assets on organization is first action to figure out actual value for asset. Besides, it is so crucial to ask a question like how much it might cost of possible threats for asset in case of not keep secure the asset.

It can be beneficial to an organization for various reasons to establish the value of assets in case of pay attention below subjects:

• Implementing effective cost-benefit analyses

• Determining specific precautions and protections

• Identifying the level of insurance scope to buying

• Finding out what asset exactly is at risk

• Obeying the rules by legal and regulatory requirements

The assets can be found on organization as intangible or tangible. Tangible asset refers firewalls, facilities, servers, laptops, and some materials. Besides, intangible asset refers brand, reputation, trademarks, intellectual property, copyrights, and data. Identifying or determining values of not tangible assets is so difficult and it changes by time.

2.3 Identifying Threats and Vulnerabilities

Likelihood of damage for assets in case of threat occurring using exist vulnerabilities on organization network and finding out impact on business can be defined as risk. In Figure 5, example risks that the organizations need to be handled in their risk management process and outcomes of possible threats are taking place. Organizations can use that information security risk management plan in their network as showed in Figure 5. There can be exist different kinds of threats that is difficult to identify in organization according to Figure 5. This unknown or new threats may be related to application and end user mistakes. For this reason, Exploring and determining and taking an action to prevent possible damages from new types of the threats related to application is so hard due to application have complicated structure. Besides, it can cause cascading errors and illogical processing in case of that issues occur. Auditing and tracking the organization network in terms of activities help to determining mistakes that is done willingly or unwillingly by human. To monitoring staff errors such as creating weak password, altering data, compromise data integrity, faulty data input on applications, organizations must implement audit periodically on their network and examine.

The organizations have to research and examine of results in terms of risk after determining vulnerabilities and threats. The risks always have possible damages for organizations. That means, the organization can loss their all assets in case of used vulnerabilities by an attacker. The damage can be like modified sensitive data, data theft, data loss, data breach, sharing confidential information, decreasing staff productivity etc. The person or team that is responsible for implementing risk analysis in organization should consider delayed loss while evaluating the harms in case of threats happened. It means that delayed loss happens after vulnerability used or occurred in organization.

Threat Agent	Can Exploit This Vulnerability	Resulting in This Threat
Malware	Lack of antivirus software	Virus infection
Hacker	Powerful services running on a server	Unauthorized access to confidential information
Users	Misconfigured parameter in the operating system	System malfunction
Fire	Lack of fire extinguishers	Facility and computer damage, and possibly loss of life
Employee	Lack of training or standards enforcement Lack of auditing	Sharing mission-critical information Altering data inputs and outputs from data processing applications
Contractor	Lax access control mechanisms	Stealing trade secrets
Attacker	Poorly written application Lack of stringent firewall settings	Conducting a buffer overflow Conducting a denial-of-service attack
Intruder	Lack of security guard	Breaking windows and stealing computers and devices

Figure 5 *Relationship of Threats and Vulnerabilities*

Delayed loss consists of the parameters like civil cases, decrease of market share, accrued delayed fines, the delayed collection of cash from customers and harm to the organization's reputation etc. For instance, when organization's critical servers like web servers are being compromised and being offline. As a result of loss or harm of asset might be broken data

integrity. And then, organization need to activated web servers again taking necessary action like implementing some remediation as software update or changing parts as hardware. If the organization wants to taking payment or sales order over their web site and in case of web servers fail and spending for hours to activate web servers again, in this case organization might lose customers, sales, profits and more during activation time period. In case of spending a week to activate web servers again, the organization will become not pay the bills and expenditures due to lack of sales and profits. That means, delayed loss occurs for organization. Depending on lose trust of customers organization might lose their business for years due to web server errors.

This situation happens rarely on organization. It's becoming so hard to calculate actual loss of an asset because of its complex issues like in case of web servers fail and taking too much time to activate. However, all these issues must take into account in terms of reflect reality for risk analysis.

2.4 Methodologies for Risk Assessment

In case of performing risk assessments in any organization, all organizations have various standardized risk assessment methodologies. Determining vulnerabilities, evaluating threats, and identifying risk values are the common elements for all kind of methodologies. However, each of risk assessments has own private study area. Responsibility of determining and performing what kind of risk assessment method will be used for organization belongs to Security Experts. The information security risk methodology enhanced and released SP 800-30 document by NIST. It is called “Risk Management Guide for Information Technology Systems” and taken into account a U.S.

federal government standard. It is generally used to determine relationship between information security risks and IT threats. The steps of this methodology listed below:

- System characterization
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendations
- Results documentation

IT security problems and computer systems issues are generally study subjects for NIST risk management methodology. It does not contain big threats such as succession planning, ecological issues, natural disasters, as how information security risks connected to business risks. It is a methodology that focuses on the operational components of an enterprise, not necessarily the higher strategic level. The methodology outlines specific risk methodology activities.

Another risk evaluation methodology is named FRAP that means Facilitated Risk Analysis Process. It is main purpose of that methodology, decreasing time and costs liability of systems that need to be evaluated using qualitative techniques. It performs preliminary risk assessments on valuable assets which need to be evaluated own method. To evaluate all systems in terms of business process or application is being used FRAP. It collects necessary data and prioritizes threats towards to busines operations according to

criticality. The person or team that is responsible, prepares required action plans in order to prevent or mitigate defined information security risks.

It might not contribute to opinion of annual loss expectancy and usage possibility numbers values. The risk management team and members define severity levels of information security risks with their knowledge. Trying to use mathematical equations to calculate of information security risk is being thought so puzzling and loss of time by author of the FRAP methodology. Holding information security assessment scope small and determining facilitated assessment processes in order to let cost effectiveness and efficiency is the main purpose in this methodology.

Other types of risk assessment methodology named OCTAVE (Operationally Critical Threat, Asset & Vulnerability Evaluation). Carnegie Mellon University's Software Engineering Institute formed this methodology. To managing information security risks personally in own organization, OCTAVE methodology is being used by the organizations. This methodology provides promoting the staff to powerful positions to taking necessary and important decisions related to which risk assessment method is the best for own organization. To turn out the actual information about what organization need and which kind of threats and risks that they are in trouble, this approach is being used in organizations due to understandable. Facilitated studies are being used by the members of risk assessment team. To understand how to implement vulnerabilities with defined threats in their organization is used facilitator, and this concept assists the members of team to understand risk methodology implementation process. It emphasizes the concept the team runs by themselves. When OCTAVE and FRAP methodology compared each other. OCTAVE assessment scope larger than FRAP methodology. While FRAP method is used to

evaluating a risk on application or system, OCTAVE is being used to evaluate all business process, IT systems and applications in organization.

FRAP, OCTAVE and NIST risk assessment methodologies only works on related to information security risks and IT security threats. Besides, AS/NZS 4360 works comprehensive on risk management than others. It is used to understand an organization's business risks, human safety, capital and financial. In spite of this methodology is being used to research information security risks, it's not only composed for this aim. Moreover, it is not work on related to information security. In this method, it is intended to remediate in terms of organization's business process.

To learn how information risk management must be implemented in the framework of ISMS (information security management system), ISO/IEC 27005 framework is used as international standard. For this reason, although NIST methodology works generally on operational and IT security ISO/IEC 27005 handle with information security problems and IT issues that are defined severity level lower than others such as information security awareness training, documentation, staff security. It should be combined with organizational information security program which overcomes against all possible information security threats.

To identify failure modes like how something on organization may fail or break and to analyze of impact of failure modes FMEA methodology is used. It provides to determining before how and where the failures will occur on organization and then it tries to take corrective precautions possible failures that will be in the future before turn into real obligations. To making great and taking good results after FMEA implementation process in organization, below steps should be considered:

1. Create a block diagram of a system or control.

2. Think about what occurs in case of each block of the diagram fails.

3. Create a table in that failures are matched with their impacts and an assessment of the impacts.

4. Fix the design of the system and set the table until the system is not known to have unacceptable issues.

5. Ensure a few experts and engineers examine the Failure Modes and Effect Analysis.

In the beginning of FMEA is enhanced for systems engineering. The first goal of this method identifies possible failures in systems, processes or products and review the procedures related to process. Recently, it is adapted to use reducing possible vulnerabilities and assessing information security risk priorities.

Besides, after organizations started to increase their understand level about complexity, variables, and detail, FMEA is being started to use for assurance risk management by organizations. It is continued to use by organizations because of need for risk awareness or culture and growing towards an operational and tactical levels.

In fact, FMEA methodology is not enough to determine or explore complicated failure modes in various systems although useful to determine failure modes in a system that is define simply in terms of complexity. For this reason, in case of determining failures in a big complex systems fault tree analysis is being used because of too much beneficial to define failures. Common operation process is implemented by Fault tree analysis method. Unwanted impact of significant case or event is defined top event on fault tree. Later, every status that has possible impact is defined on tree as rationale phrase. Even, to define possible failures real numbers are added on fault trees with labeling method. To

calculate possible failures using fault tree's data is generally is used by computer software tools.

All possible faults and threats which may happens should be registered correctly in fault tree. To categorize the types of threats like hardware failure, component failure, internet threats, physical threats, network threats, related to software threats may be defined on branches of the tree. After all feasible categorize on branches that is defined, organization can cut branches of tree as defined unnecessary in a specific system. Usually, if the systems can't reach to internet directly, organization can cut related branches of the tree.

Well-known software failure cases or events which may be discovered listed below obtained from fault tree analysis method:

- Valid however unexpected outputs
- Sequencing or order
- Insufficient error handling
- False alarms
- Incorrect timing outputs

In fact, because of the complexity of software and heterogeneous environments, this is a very small list.

Just in case you do not have enough risk assessment methodologies to choose from, you can also look at CRAMM (Central Computing & Telecommunications Agency Risk Analysis & Management Method), which was created by the United Kingdom, and its automated tools are sold by Siemens. It works in three distinct stages: define objectives, assess risks, and identify countermeasures. It is really not fair to call it a unique

methodology, because it follows the basic structure of any risk methodology. It just has everything (questionnaires, asset dependency modeling, assessment formulas, compliancy reporting) in automated tool format.

Similar to the "Security Frameworks" section that covered things such as ISO/IEC 27000, CobiT, COSO, Zachman, SABSA, ITIL, and Six Sigma, this section on risk methodologies could seem like another list of confusing standards and guidelines. Remember that the methodologies have a lot of overlapping similarities because each one has the specific goal of identifying things that could hurt the organization (vulnerabilities & threats) so that those things could be addressed (risk reduced). When these methodologies compared each other, they are all not similar in terms of their unmatched issues and uniqueness methods. Organization should track OCTAVE or ISO/IEC 27005 methodologies to implement organizational information security risk management process and combine with own up to date security program. In case of the organization wants to work on just IT security risks during assessment process, organization may implement NIST 800-30 method on their network. In case of the organization has insufficient budget and need to work on only specific system or process during assessment process organization may implement FRAP (Facilitated Risk Analysis Process) method. In case of the organization wants to investigate negative results deeply when a security risk is occurred, organization can implement fault tree or FMEA (Failure Modes and Effect Analysis). In case of organization need to comprehend own business risks, organization may use AS/NZS 4360 methodology.

2.5 Risk Analysis Approaches

There are two methods that are used as qualitative and quantitative for risk analysis process in organizations. To define all assets as numeric and monetary during risk analysis process, organizations use quantitative risk analysis method. To identify total risk and residual risk all items in analysis such as probability items, safeguard effectiveness, threat frequency, impact damage, asset value, uncertainty, severity of vulnerability and safeguard costs are used. When quantitative method compared with qualitative, it uses some further mathematical equations and scientific methods than other. In the qualitative risk analysis "softer" methods on related items is being used compared with quantitative method and determining to amount of the data is so hard in this approach. For this reason, data elements or all asset items might not be defined as numeric values to use in mathematical equations. For instance, in case of buffer overflow occurred on organization's critical web server, organization can have loss of risk $60000 and in case of database threat issue occurred organization can have loss of risk $15000 and in case of FTP (File transfer protocol) server threat occurred organization can have loss of risk $6000. The results and evidence might not be defined as financial values in the qualitative risk analysis. However, the risks could be classified color in Green, Red and Yellow. To estimate the severity level of financial losses and determine every possible threat quantitative risk analysis method is being used in organizations. Mathematical equations could not be used in qualitative risk analysis method. Besides, it evaluates the risks in terms of ideas and scenarios and risk severity level. To do this, it uses rating approach with colors. In some situations, two types of approaches are being used according to their suitability in organization and there are own advantages and disadvantages. To decide what method will be the best option, organization

management or responsible team should decide which tools are necessary and then related tools will determine the type of approach.

2.5.1 Automated Risk Analysis Methods

If the data that need to be included for risk analysis in mathematical equations is gathered manually and wanted to correctly evaluation. This might be so hard for organization. To avoid this situation and interpret more precisely, organizations can use automated risk analysis software or tools that have various options from the market. To optimizing time-period needed for become reusable the data and to finish further analyses automated risk analysis tool can help the organization. Besides, to present to detailed reports and graphs to management this type of risk analysis might be so useful.

Implementing calculation fast and forecasting coming expected losses and determining influences and advantages of selected precautions decreasing an effort that is done manually are main purpose of tools. To demonstrate what results will be with various metrics when possible threats occurred, sensitive information is sent to related database to run a few scenarios by automated risk analysis tools. For instance, in case of fire occur in organization, to calculate possible results automated tools are rerun a few times with various metrics after tool gathering necessary data. In case of a virus damage possible loss of 50 percent of the critical data on FTP (File Transfer Protocol) file server. In case of hacked four database that contains customer credit card information how much the organization will lose in terms of financial. So, automated risk analysis tools provide an information to organization to better understanding possible risks and about which risks should be handled first according to their severity level and probability of risk.

2.6 Steps in Risk Assessment

2.6.1 System Characterization

Determining sensitive or critical information for organization is so crucial thing defining the elements of system like transactions, staff, network devices, software, rules patches, hardware, policy, asset values etc. in terms of assisting the storage, transfer data, processing of information. This is often referred to as the information technology (IT) system. This is generally called the IT (information technology) system. So, the whole information technology components must be identified as value of assets, equipment, flow of information, and staff responsibilities such as, using strong password and periodically change it for security, lock computers against unauthorized access, not use USB drives that contains suspicious software, not open the URL links that come from unknown resources and attend information security awareness trainings in organization etc.

System characterization can be completed with some combination of face-to-face staff interviews, surveys, visiting periodically organization, and automated or manually scanning tools. Many types of scanning tools are available such as OpenVAS, NetScanTools, iNetTools, Strobe, Netcat, Nmap and Winscan etc.

2.6.2 Threat Assessment

Designing a defense strategy is not feasible unless understand what to defend towards (Decker, 2001). Each of threat has possible problem, damages and negative effect to the information technology sources. Defining feasible reasons or root cause of threats is a great advantage for organizations. When a malicious attack occurred, it is thought due to human error first. However, main reason may not be this. Reasons may also be natural disasters like bad weather conditions, landslides, floods, hurricane avalanches, tornadoes, and earthquakes, etc. Besides, main reasons may be elements in the environment, like electric energy failures.

The most dangerous threats can be defined internal threats that is done by human. For this reason, threat intelligence and the strategy manage malicious attacks using gathered information about internal threats. There may not be malicious aim of internal threats which is done by human. As an example, a threat may be originated from not vigilant or negligence like not change password periodically and forgetting computer login username and password information on desk that will be able to see by everyone. Besides, it can be unintentionally downloading malicious computer software because of phishing attacks or accidentally creating a rule on firewall to allow unwanted traffic.

It is so hard to categorize malicious attacks that is done human hand due to their mistakes and motivations differences (McClure, Scambray, & Kurtz, 2001). Human attackers usually are defined as internal and external threats for organization. The classic internal attacker can be defined dissatisfied and crooked staff that asks vengeance from organization or theft another staff's individual or sensitive data. So, the most dangerous attack can be defined as internal attackers. Because internal attackers have authorized

permission and access to an organization's worthy assets. Besides, they likely have domain accounts that is identified high privileges like local admin, windows admin or domain admin etc. On the other hand, external attackers to gain access must attack to target organization’s defenses (like IPS, IDS, VPN servers, 2FA servers, antivirus, firewalls). They will probably difficulty gaining access by domain admin, root, local admin privileges because of these defenses. External attackers can define amateur “hackers” encouraged with interest, overconfidence or curiosity, professional criminals seeking for benefit or steal sensitive data, terrorists looking damage or violence, soldierly agents encouraged with national interests, or industrial agents targeting to steal sensitive or critical data. External threats may also contain malicious software, DOS (Denial of Service) attack, DDOS, phishing attack, worms, viruses like trojans, that spread with themselves via Internet. Besides, defining significant external threats is generally possible, however a probability always exists for a new unnamed like zero-day malware obscure external threat.

2.6.3 Vulnerability Analysis

Vulnerabilities should be considered while cyber threats evaluated. Taking access authorization to the system and implementing unauthorized activities on a specific server or computer by an attacker using some weakness on a system can be characterized as vulnerability. In case of related system in organization is not vulnerable against possible threats, any threat is not crucial for organization. As an example, in case of windows 10 has buffer overflow vulnerability, it will not be crucial thing due to organization does not have any Windows 10 laptops or computer.

To define technical vulnerabilities is the effortless one. Suppliers of hardware and network device generally release known vulnerabilities, bugs and up to date patches for own products. Besides, a few web sites like CERT (http://www.cert.org/advisories) and BugTraq (http://www.securityfocus.com/archive/1) publish well-known vulnerabilities with security some suggestions. To evaluate operational system in organizations automated vulnerability scanning software or apps as Nessus, Burp Suite, Beyond Security, Satan and Acunetix is being used widely. Besides, all these scanners have a database which contains common vulnerabilities that is known by everyone. System and network are tested for identified vulnerabilities by scanner tools. As another method to discover vulnerabilities or activities on a likely possible target system attack simulation method is being used to simulates abnormal actions that is triggered by an attacker (NIST, 2003). Finding weaknesses in possible target system using active attacks is the main purpose.

It is not possible to know all vulnerabilities in a likely target system. Vulnerabilities can take place because of security management. For instance, human resources may be inadequate to meet all significant security responsibilities or can be lack of trained staff. Security policies may not be up to date, exposing the target system to likely compromise. Other vulnerabilities may be related to system transactions. For example, if we think used USBs are disposed in trash which is directly reachable. Taking back discarded data would be easy for everyone.

2.6.4 Impact Analysis

The effect of every cyber-threat on the target organization count on some obscure elements and the probability of the threat taking place and the damage because of successful compromise and the density of iteration of the cyber-threat. In reality, these elements can be hard to estimate, and there are a lot of route to predict and assemble them in an effect anatomy. The impact analysis may be defined as qualitative (descriptive) and quantitative (mathematical). To define all assets as numeric and monetary during risk analysis process, organizations use quantitative risk analysis method. To identify total risk and residual risk all items in analysis such as probability items, safeguard effectiveness, threat frequency, impact damage, asset value, uncertainty, severity of vulnerability and safeguard costs are used.

When quantitative method compared with qualitative, it uses some further mathematical equations and scientific methods than other. In the qualitative risk analysis "softer" methods on related items is being used compared with quantitative method and determining to amount of the data is so hard in this approach. For this reason, data elements or all asset items might not be defined as numeric values to use in mathematical equations. For instance, in case of buffer overflow occurred on organization's critical web server, organization can have loss of risk $80000 and in case of database threat issue occurred organization can have loss of risk $20000 and in case of FTP (File transfer protocol) server threat occurred organization can have loss of risk $8000. The results and evidence might not be defined as financial values in the qualitative risk analysis. However, the risks could be classified color in Green, Red and Yellow.

To estimate the severity level of financial losses and determine every possible threat quantitative risk analysis method is being used in organizations. Mathematical equations could not be used in qualitative risk analysis method. Besides, it evaluates the risks in terms of ideas and scenarios and risk severity level. To do this, it uses rating approach with colors.

When consider qualitative and quantitative concept, both has some advantages and disadvantages. In some cases, it is implemented according to availability. The management or team that is responsible will choose appropriate concept to implement on their network with the help of tools they select to use.

If we choose to carry out a quantitative analysis, then we are going to use mathematical equations for our data interpretation process. The most commonly used equations used for this purpose are the single loss expectancy (SLE) and the annual loss expectancy (ALE).

The SLE is a dollar amount that is assigned to a single event that represents the company's potential loss amount if a specific threat were to take place. The equation is laid out as follows:

Asset Value × EF (Exposure Factor) = SLE

The exposure factor (EF) represents the percentage of loss a realized threat could have on a certain asset. For example, if a data warehouse has the asset value of $150,000, it can be estimated that if a fire were to occur, 25 percent of the warehouse would be damaged, in which case the SLE would be $37,500:

Asset Value ($150,000) × Exposure Factor (25%) = $37,500

This tells us that the company can potentially lose $37,500 if a fire took place. But we need to know what our annual potential loss is, since we develop and use our security budgets on an annual basis. This is where the ALE equation comes into play. The ALE equation is as follows:

SLE × ARO (Annualized Rate of Occurrence) = ALE

The ARO (annualized rate of occurrence) is the value which indicated the forecasted frequency of a specific possible threat occurring during 12-month time-period. The range may be from 0.0 (never) to 1.0 (once a year) to greater than 1 (a few times a year) and anywhere in between. As an example, in case of the likelihood of a fire occurring and damaging organization's data warehouse is once every ten years, the ARO (annualized rate of occurrence) value is calculated as 0.1.

Consequently, in case of outbreak of fire in organization's data warehouse facility it may reason $37,500 in harms, and the periodicity of annualized rate of occurrence of outbreak of fire has an annualized rate of occurrence value 0.1(calculated once a decade). Later, annual loss expectancy (ALE) value is calculated as $3,750 ($37,500(damage) × 0.1(ARO) = $3,750).

When the organization or company requires to keep secure their assets against possible threat like fire, annual loss expectancy (ALE) value says that, if you want to provide enough secure your network you should allocate a budget $3,750 or less for that every year. Understanding actual probability of threats and how much will give damage for organization, it is so crucial in terms of determining how much organization will

allocate a budget to prevent towards possible threats. For this reason, allocating a budget more than $3,750 per year is not sensible in terms of business.

Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)
Facility	Fire	$230,000	0.1	$23,000
Trade secret	Stolen	$40,000	0.01	$400
File server	Failed	$11,500	0.1	$1,150
Data	Virus	$6,500	1.0	$6,500
Customer credit card info	Stolen	$300,000	3.0	$900,000

Figure 6 *Values of a quantitative risk analysis*

As demonstrate the result of a quantitative risk analysis in Figure 6. When the organization consider the results of risk analysis report. Organization may take right decisions about probability of risk occurring, which threats should be handled first according to its severity, how much might be damage cost in case of threat occurred. Besides, the organization learns from this analysis how much budget should be allocated to prevent possible threats. This would cause to taking right decisions about business process in favor of organization, managing budget correctly without purchasing unnecessary security tools and seeing of the big picture.

According to Figure 6, in case of data breach on organization system due to virus leakage. The budget must allocate up to $6500 by organization in order to prevent possible loss with necessary tools like antivirus software, EDR (Endpoint detection and response) software.

As an alternative types of risks analysis can be defined qualitative method. Defining numbers, determining the values of an assets in terms of losses and components is not

identified using qualitative method. This method provides to determine various types of probability of risk and severity of the threats and taking place the necessary precautions according to views. Besides, the qualitative risk analysis can contain dozens of scenarios. The qualitative risk analysis consists of experience, perception, judgment and most commonly used practices. To collect necessary data using qualitative techniques such as interviews, face to face meetings, storyboarding, questionnaires, brainstorming, focus groups are used. The team or person that is responsible for risk analysis in organization must decide best technique that will be able to use against possible threats which need to be evaluated, considering culture of organization and staff that is included in analysis.

Responsible team in organization bring together all well-educated, conscious and experienced staff to evaluate possible threats. Every staff gives an idea to the organization with their perspectives about probability of threat occurrence and possible loss of damages in case of present a scenario which is defined possible threats and loss of damage.

Organization uses all scenarios of defined vulnerability and doing research about how to benefit from it. An expert that is know all threat scenarios in organization must examine the scenarios to understand how to possible threat can be occurred. Later, precautions to reducing of damage for threats is assessed and related threat scenario has been performed for each protection measure. The probability of risk occurrence and likelihood of loss of damage may be sequenced as low, medium and high on a level of 1 to 10 or 1 to 5. In Figure 7, mostly used qualitative risk matrix is demonstrated. The person that is responsible for analysis determines rank the probability of threat occurrence and the possible loss of damages and cons or pros for each precaution and prepares the reports with this information about how to enforce best solutions to prevent possible threats. Later,

according to prepared report is presented to senior management to taking right decisions or actions.

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Figure 7 *Qualitative risk matrix. Likelihood versus consequences (impact).*

Impact analysis provides to organization contribution in terms of rating the risks, protecting strengths, determining weaknesses, providing communication between members of the team and presenting reports and thoughts for these issues by the person or experts that know.

A scenario is presented a report by risk analysis team defining the threat that access to five file servers that contains sensitive data by attacker. Later, that scenario report is delivered to team of five members that is responsible such as operational manager, system administrator, IT manager, application programmer and database administrator, besides given a sheet that contain severity level of threat, loss potential and every precautions' effectiveness.

All these are rated from 1 to 5 and 1 number means least severity, effectivity, and probability of the threats. Outputs of the risk analysis report demonstrate in the Figure 8.

Threat = Hacker Accessing Confidential Information	Severity of Threat	Probability of Threat Taking Place	Potential Loss to the Company	Effectiveness of Firewall	Effectiveness of Intrusion Detection System	Effectiveness of Honeypot
IT manager	4	2	4	4	3	2
Database administrator	4	4	4	3	4	1
Application programmer	2	3	3	4	2	1
System operator	3	4	3	4	2	1
Operational manager	5	4	4	4	4	2
Results	3.6	3.4	3.6	3.8	3	1.4

Figure 8 *Qualitative Analysis*

Risk analysis team should prepare a report with compiled data and submitted to management. In case of the team submit a report to senior management and organization will see significance of measures to be taken by personnel than buying a next generation firewall or installing a honeypot system or IDS (intrusion detection system) or IPS (Intrusion prevention system).

It is the outcome of a threat that is known by management. Senior management are going to observed probability, severity, damages of possible every threat, thus management will be able to determine the reasons of risk evaluating the risks and which threat will be able to handle initially.

2.6.5 Risk Determination

To calculate cyber-threat risk level, its likelihood of risk must be multiplied with the impact of risk.

$$\text{Risk} = \text{likelihood} \times \text{impact}.$$

The risks that have high likelihood and high effect can be defined as critical risks. A high impact threat with a too low probability might not be noteworthy, and in the same way, a highly probably cyber-threat by low impact can be defined as less important. By a software tool of likelihood and impact, entire cyber-threats can be defined according to threat grade. As an example, a basic grading output can be high, medium, or low risk. Risk levels can be rated using from 0 to 10 ranking method (NIST, 2002).

The levels of risk demonstrate the priority of related risk. High critical risks have to be defined the most important and most urgency in the following phase of risk mitigation. Medium risks have to be defined by risk mitigation however probably by less urgency. In the end, low cyber-risks could be admissible without apply risk mitigation procedure or can be reduced if organization has enough sources.

2.7 Risk Analysis for A Case Study

2.7.1 Risk Assessment Approach

The organization is figured out assets, critical threats, vulnerabilities, and risks effect using Qualitative Assessment method by elaborated Risk Analysis framework in this section. Possible reason of an incident which might cause to damage to organization assets can be defined as cyber-threat. Vulnerability can be defined as weakness of organization's valuable assets which can be damaged due to cyber-threats. Besides, Impact can be calculated after information security incident occurred on organization's valuable assets. (ISO/IEC:13335 2004; ISO/IEC, Guide 73 2002; C. Mike, S. David, M. ,. James & G. Darril, 2018). To determine possible cyber-threats, vulnerabilities, and impact after implemented necessary security controls on organization's network can be used risk assessment approach. Table 1(Asset values and Incident Matrix) is being used to define qualitative value of valuable assets of an organization that is affected by information security incidents. To identify possible recurrence period of cyber-threats and probability of vulnerability is being used Table 2(Threats and Vulnerability Likelihood). Moreover, it is not being used any risk assessment standard for this study in the tables that contains some values. So, comments about risk assessment are being made according to organization's requirements. Responsibility belongs to the asset owners to gathering correctly cyber-threats information and possible vulnerabilities for all valuable assets defined for organization in this study. Besides, Liability about risk assessment results like values of an assets in Table 3 belongs to both of supplier and asset owners.

LIKELIHOOD	DESCRIPTION	INTERPRETATION
1	Negligible	Once every 1000 years or less
2	Extremely Unlikely	Once every 200 years
3	Very Unlikely	Once every 50 years
4	Unlikely	Once every 20 years
5	Feasible	Once every 5 years
6	Probable	Annually
7	Very Probable	Quarterly
8	Expected	Monthly
9	Confidently Expected	Weekly
10	Certain	Daily

Table 2 *Threats and Vulnerability Likelihood Table*

RISK LINE	ID No.	Assets	Owner	Values (A)	Threats	Likelihood (T)	Vulnerabilities	Likelihood (V)	Risks (A*T*V)
ABOVE RISK APPETITE	16	Electronic Data	CIO	5	Human error	8	Mental Stress	9	360
	18	Electronic Data	CIO	5	Human error	8	Employees Physical fatigue	9	360
	17	Electronic Data	CIO	5	Human error	8	Fear to Consult	8	320
	14	Electronic Data	CIO	5	SQL Injections	6	Execution of malfunctioned queries irrespective of warnings	9	270
	15	Electronic Data	CIO	5	SQL Injections	6	Outdated DBMS	9	270
	2	Reputation	CEO	5	Data breach	6	Existence of backdoor	8	240
	7	Ruputation	CEO	5	Fraud	6	Disgruntled employees	8	240
	13	Electronic Data	CIO	5	SQL Injections	6	Bad coding Designs	8	240
	1	Reputation	CEO	5	Data breach	6	Outdated Security Software	7	210
	3	Reputation	CEO	5	Data breach	6	Reliance of reputation on trust	7	210
	25	Revenue Management System	CIO	3	Cross-Site Scripting	7	Susceptibility to Malicious code	10	210
	27	Revenue Management System	CIO	3	Cross-Site Scripting	7	User input support through input field	10	210
	4	Reputation	CEO	5	Misuse of resources	6	Staff dishonesty	6	180
	5	Reputation	CEO	5	Misuse of resources	6	Unclear resources utilization guidelines	6	180
	6	Reputation	CEO	5	Misuse of resources	6	Poor resource management	6	180
	8	Ruputation	CEO	5	Fraud	6	Unclear System Access Clearance guidelines	6	180
	9	Ruputation	CEO	5	Fraud	6	Staff dishonesty (Integrity loss or failure)	6	180
	11	Electronic Data	CIO	5	Data theft	6	Disgruntled employees	6	180
	12	Electronic Data	CIO	5	Data theft	6	Disposal of Storage media without proper erasure	6	180
	26	Revenue Management System	CIO	3	Cross-Site Scripting	7	Support for various unsafe scripting technologies.	8	168
	34	IT Hardware	CIO	2	Power interruptions	9	Inability to operate without power supply	9	162
	36	IT Hardware	CIO	2	Power interruptions	9	Fluctuating power supply (Unstable Power Supply)	9	162
	37	Staff	COO	2	Social engineering	9	Human tendency to be gullible (getting something for nothing)	9	162
	38	Staff	COO	2	Social engineering	9	Inclination for immediate gratification	9	162
					RISK APPETITE				150
BELOW RISK APPETITE	39	Staff	COO	2	Social engineering	9	Inclination to Improved status gain	9	162
	23	Revenue Management System	CIO	3	Stack-Overflow attacks	6	Weaknesses in the programming language used to develop the systems	8	144
	24	Revenue Management System	CIO	3	Stack-Overflow attacks	6	Zero-day vulnerabilities	8	144
	35	IT Hardware	CIO	2	Power interruptions	9	Inability of backup power (UPS) to sustain long hours	8	144
	19	Revenue Management System	CIO	3	Denial Of Services	6	Low Memory Resources	6	108
	20	Revenue Management System	CIO	3	Denial Of Services	6	Limited Bandwidth	6	108
	21	Revenue Management System	CIO	3	Denial Of Services	6	Protocols in use such as Telnet	6	108
	22	Revenue Management System	CIO	3	Stack-Overflow attacks	6	Bad coding habits	6	108
	42	Staff	COO	2	Illness (Health)	7	Illnesses due to change of weather	7	98
	10	Electronic Data	CIO	5	Data theft	6	Breaching legal requirements	3	90
	28	IT Hardware	CIO	2	Heat	6	Susceptibility of Equipments to temperature variations	7	84
	30	IT Hardware	CIO	2	Heat	6	Susceptibility of Solder joints to melt at high temperatures	7	84
	40	Staff	COO	2	Illness (Health)	7	Weak immune systems due to genetic variations	6	84
	41	Staff	COO	2	Illness (Health)	7	Incomplete Immunisation to Common Diseases	6	84
	43	Staff	COO	2	Accidents	6	Ignorance to Precautions	7	84
	44	Staff	COO	2	Accidents	6	General carelessness and forgetfulness	7	84
	45	Staff	COO	2	Accidents	6	Tendency to take risks, being fearless	7	84
	29	IT Hardware	CIO	2	Heat	6	Susceptibility of Processor Chips to melt at high temperatures	6	72
	31	IT Hardware	CIO	2	Humidity	4	Non-water resistant Equipments	8	64
	33	IT Hardware	CIO	2	Humidity	4	Susceptibility to short circuiting due to water/moisture contact	7	56
	32	IT Hardware	CIO	2	Humidity	4	Susceptibility to corrosion due to rusting	5	40

Table 3 *Risk Assessment Register (the different assets in color code)*

2.7.2 Risk Appetite

Risk appetite concept is the quantify and kind of risk which is ready to pursue, keep or receive (ISO:31000 Risk management, 2018). Besides, risk appetite is determined by the organization management.

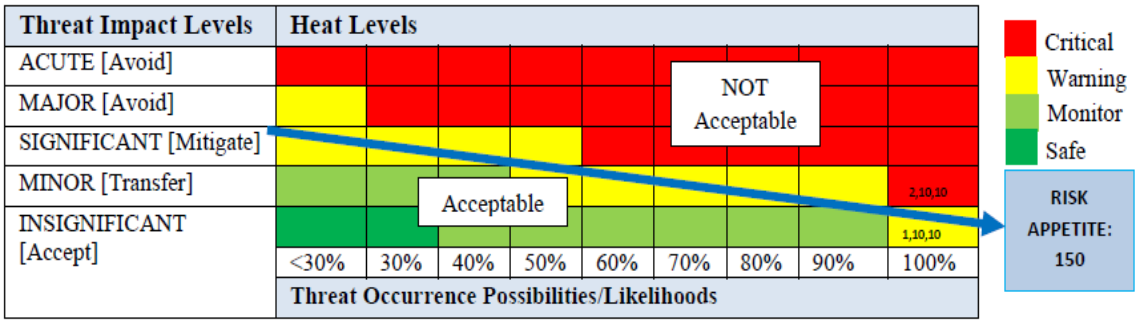

Table 4 *Risk Register heat map*

Table 3(Risk assessment or register) is being used to determine heat map. Later, this heat map is being shared with organization management to identify risk appetite. The risk appetite score is being defined between (asset, threat, vulnerability) values (1, 10, 10) and (2, 10, 10) that answer to risks same to 100 and 200 one by one for this organization. According to heat map, risk appetite is being calculated as 150. If cyber-threats over risk appetite's value, that is not admissible and should be refrained and taken the control. If that value under risk appetite's value, it is admissible and ignorable in terms of risks and should be subjected ISM (Information Security Management) rules and policies of organization. Organizations must refrain and destroy the threats that is classified color in RED. Threats that is sorted color in YELLOW can be mitigated by risk mitigation policies. Minor threats that are demonstrated color in GREEN can be transferred to third party. Besides, unimportant threats should be tracked by organization.

2.7.3 Impact Controls

Organizations need to necessary controls periodically to handle and manage defined risks (W. Michael & M. Herbert, 2010). It needs to precaution plans and controls must be identified to change risks and resist against the threats for organization. Controls that are completed by organization may be used to getting rid of data breach, security incident, compromise. Besides, it can be used to detect, mitigate, prevent and deflect too. The organization probability for damage is named risk (C. P. Pfleeger & S. L. Pfleeger, 2011). To identify necessary controls according to organization needs and sources can be used ISO/IEC 27001 standard. Industry standards and implementation rules may be defined organization's sources. Decisions regarding to information security controls must be balanced by risks and sources restrictions because of lack of organization's purchasing power to manage, maintain and install costly security controls and connected systems. The risk control list that is defined by organizations is going to modify risks which is defined in the risk assessment stage. Thus, both of defined control list is going to work harmoniously to mitigate the risks. Besides, it's so important to check if latest controls disagreement by exist controls or not or how efficiently they are going to work in common to applied risk controls by organization.

Risk assessment components in Table 3 are indicated Reputation, Revenue Management System, Personnel as critical assets and Electronic Data. The purpose of created risk assessment using defined controls is executing the best action plan and techniques to prevent against specific threats. Technical, physical and administrative that is defined three types concept as control precautions is being accepted. To detailed

tracking, efficient controls, physical security, protective technical precautions, regenerative, inhibitive techniques the best option to determining particular security risk policies is using integrated ISO270001 and NIST combination. For this reason, varied controls precautions are being adopted below to mitigate, eliminate, transfer or permit the information security risks in terms of powerful information security embraced least Privilege, separation of duties security principles and Defense in Depth security.

Least Privilege Security: no actions, connections or communications without permission and need (W. Evan, Security Risk Management, 2011).

Defense in depth Security: use of security techniques options or alternatives of control to mitigate exposure in case of security control endanger (W. Evan, Security Risk Management, 2011).

Separation of Duties: decrease mistakes and do it so hard to exploit access privileges for individual benefits (W. Evan, Security Risk Management, 2011).

Administrative Controls

These types of controls are named "soft controls" such as job descriptions, roles, responsibilities, visitors or guest records, alteration control, penalty for undesired cases, user registration. To create accurately information security culture in organization some typical rules and policies is defined such as Secure Data Transmission Policy, Clean desk policy, Encryption method policy, Digital signature acceptance policy, Password protection and construction policy, data lifecycle policy, Data breach policy, Ethics policy, Security incident response plan policy, Email policy (like determining phishing email),

Disaster recovery plan policy, Non-disclosure agreement for service providers. To mitigate risks to acceptable level especially related to IT systems should be determined Acceptable Use Policy (AUP) on organization. Besides, all defined policies are going to be improved the system process providing entire information security management, human mistake check and social engineering. The policies that are defined by organization must be checked once two years. Besides, Information security awareness training should continue in organization. Moreover, to check staff's past job experience or evaluate talented staff in hiring process must identify outlines and regulations as an administrative control. After all, Separation of duties and Job rotations and Data classification or labelling should be embraced by organization.

Technical Controls

Organization network infrastructure must be made safe to prevent cyber-attacks with latest technologies such as Demilitarized Network Zones, patch management, Intrusion prevention systems (IPS), Next Generation Firewalls, URL filtering, Virus scanner tools, antispyware, App filtering, Intrusion detection systems (IDS), Data Leakage Prevention (DLP), Attack simulation tools. To manage or control personnel access to organization's sensitive data must be applied data encryption method by organization to ensure role-based access, data confidentiality and account management control also to access organization network remote Virtual Private Networks (VPNs) and Two Factor Authentication(2FA) like SMS verification. Besides, unusual activities or actions in network should be monitored checking audit logs by organization and organizations must check the data backups, server software images for fail recovery.

Physical Controls

Organizations should use locks, IRIS scanner, identity card and finger-print verification to ensure detective and deterrent controls for data center, camera room, security guards to prevent unauthorized access to organization's physical assets. Besides, using Uninterruptible Power Supply (UPS) products in organization's data center can prevent power failure. Thus, IT hardware may not be negatively influenced because of power failure.

2.7.4 Compensating Controls

To mitigate the risks to acceptable level according standards can be used a compensating control. However, this control might not be paired with estimated control that is defined in the standards. (W. Evan, Security Risk Management, 2011). It is well known fact that, organizations sometimes might not be completely accomplished control objectives. So, risks of unexpected in the organization activities might happen. For this reason, organization should enforce extra controls to mitigate risk lowest level also assess the cost-benefit for organization future (F. T. Harold & K. Micki, Information Security Management Handbook, 2007). Compensating controls consist of Physical elements, Technical, Logical and Administrative like mentioned before.

2.7.5 Residual Risks

Residual risk can be defined as remaining quantity of risks on organization that is exposed following enforced the suggested controls. Residual risk can be calculated as explained previous chapters. Anymore, the risk report that contain how to mitigate risk to lowest level in organization with suggested controls can be presented to management (W. Evan, Security Risk Management, 2011). Later management should take an action to prevent possible risks according to report.

3. RISK MITIGATION

It can be supposed that likely target organization is going to have not sufficient sources or allocate a budget to security. For this reason, sometimes it might not be possible to protect regarding to potential cyber-threats. Besides, a definite category of risk can be admissible by likely target organization. In the operation of risk mitigation is to fund restricted sources to change inadmissible risks into agreeable ones. Risk mitigation process can be originated from technical and nontechnical replace. Technical replaces cover security equipment (VPN parameters, access controls, firewalls, data leakage prevention, intrusion detection systems, physical security, intrusion prevention systems, antivirus software, audit trails, backups etc.) and governance of that equipment. Defining policy replacement, user instruction, and end user information security awareness can be defined as non-technical replacements. Reviewed the risk assessment analysis process, cyber-risks may be supposed or mitigated. Risk approach expresses to risks which are selected to be admissible. Admissible risks are usually low level of risk however a mindful cost-benefit

analysis must be completed to determine which risks to admissible. In case of risk mitigation process applied, Likely target organization will have of various choices. (NIST, 2002):

- Risk avoidance tries to remove the reason of risk, as an example, removing the probability or vulnerability the of the threat. As an example, widespread vulnerabilities can be fixed by implementing latest policies, firewall rules, configurations, and patches. Well-known all over the world risk checks works to mitigate the probability of a cyber-threat. Protective checks aim to destroy vulnerabilities and, in this way avoid successful cyber-attacks.

- Risk restrictions try to mitigate the risk to an admissible grade by performing controls to mitigate the impact or estimated frequency. As an example, firewalls, IPS, IDS, DLP, PAM access controls, NAC (Network Access Control) and may be hardened to perform it so hard for external cyber-attackers to unauthorized access to likely target organization's network. Remedial checks mitigate the impact of cyber-attack. Hardened audit checks explore types of cyber-attacks and launch remedial controls.

- Risk transference means reallocating the risk to different side. The most widespread and familiar practice need insurance, that lets likely target organization to prevent the cyber-risk of potentially significant and great damage in place of a constant loss. Risk mitigation steps are demonstrated in Figure 9.

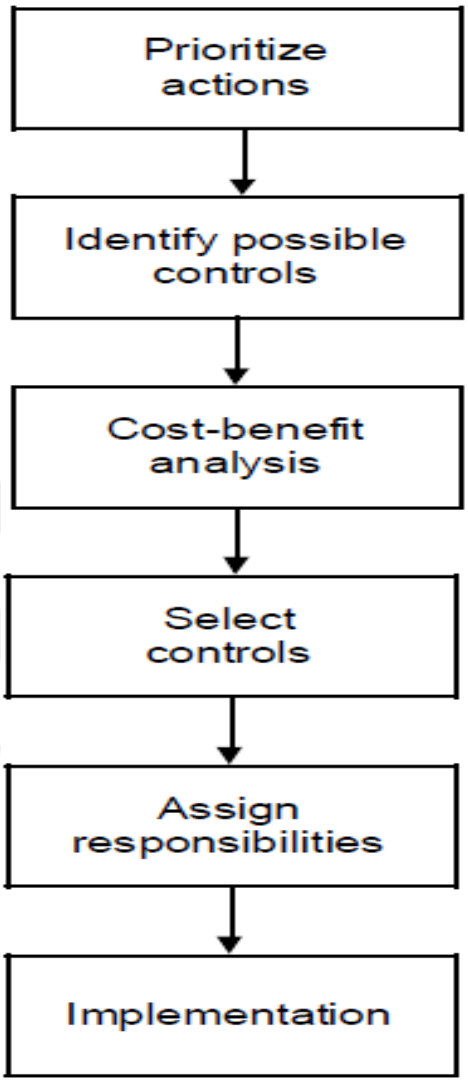

Figure 9 *Steps in risk mitigation.*

3.1 Prioritize Actions

The level of cyber-risks by their defined during the risk assessment process is going to recommend which precautions must be engaged. Absolutely, the risks by inadmissible high levels must be handled with the largest urgency. The list of necessary actions to handle the described risks must identified during this process.

3.2. Identify Possible Controls

This step analyzes all feasible action plans to reduce risks. Some checks will be more possible or cost powerful than others, however that fixing is let for next stage. The conclusion of this step will shed light to next control list.

3.3 Cost-benefit Analysis

The purpose of risk mitigation is resolved of trade-offs between costs and profits connected to all control option (Gordon & Loeb, 2002; Mercuri, 2003). Cost-benefit analysis process defines that likely target organization's sources are restricted and have to be spent by cost-effective approach to mitigate risks. A checklist is valuable just if its cost can be verified by the decrease in the grade of risk. The cost of risk may not be so easy to define. Hardware and software that are identified as tangible things costs are obvious. Besides, there can be costs for staff awareness training, time, extra human resources, and policy fulfilment. A checklist may also affect the performance of the IT (information technology) system. As an example, audit outputs are valuable for tracking system-level activities like password change, login credentials on servers and clients however could

slow down efficiency of system performance. That situation is going be created an extra expense hard to estimate.

Budget and time that is need always limited for organization. Organizations usually have a long risk list that contain possible risks after finish information security risk evaluation. However, organizations need to rank all risks to determine which threats will be able to acceptable and which threats can be easily reduce using technical method. Generally, cost benefit analysis was being used for determination of which threats will be able to acceptable doing a cost benefit analysis and allocate a budget for every damage or loss, protection cost towards possible threats, identifying of probability of loss. Later, it was being used to determining outweighs whether protection cost towards possible threats than benefit.

Mathematical equations and scientific processes that are used for Risk assessment and Cost-benefit analysis is produced so much numerical data. But making sense of this numerical data can costly and need some time. The outcomes of numerical data usually faulty and tentative.

The Cost of Loss

It can be so hard to identify cost of damage or loss. To calculate cost of replacing or repairing for specific product is simplest one of calculation. The complex calculation of cost may take into account of cost of out-of-service hardware, the cost of awareness training for staff, the cost of other things like procedures originated from loss, the cost of organization's reputation and organization's customers. Defining more parameter in the

cost of calculation is going to be increase accuracy of the calculation besides, organization's struggle at the same time.

The risks that are defined for organization doesn't need to be defined a value. Defining a cost limit is enough for each loss of risk firstly. As an example, the loss of hard disk can be defined cost limit like "under $1000," in case of devastating fire occurred in the data center can be defined cost like "over $2,000,000." In fact, some of assets can be classified as "irreparable/irreplaceable". All these can contain some issues like loss of organization's all critical assets or passes away of the personnel who is work for organization.

Organization can ask to assess loss of risk using more sensitive scale than defining the assets or items as "lost/not lost" category. As an example, organizations can ask to define different costs listed below:

- Unauthorized disclosure to strangers, competitors, and the media
- Unauthorized disclosure within the organization
- Unauthorized disclosure to some outsiders
- Intentionally or unintentionally partial loss or damage
- Non-availability over a medium term (1-2 weeks)
- Non-availability over a short term (< 7-10 days)
- Non-availability over a long term (more than 2 weeks)
- Permanent destruction or loss
- Recovery or Replacement cost

The Probability of a Loss

Organization needs to forecast the probability of threat happening after defined possible threats. It is the simplest one to forecast yearly for these threats.

It is so difficult work to scaling the probability of occurring a risk. Sometimes, organizations can take some suggestions from third party companies like insurance or audit firms. In case of the threat occurs regularly, organization can move looking own log history. Besides, organizations can be taken of advantage from released the reports that contains some statistic information about threats. Organization can create an estimation using own experience and learnings from issues that are occurred before. As an example:

- To formal guess of probability of occurring power cut along to year in organization, power company can help about the estimation. Besides, organization can calculate or scale power cutting time as seconds, minutes, or hours.
- Organization may calculate likelihood of passes away of the personnel evaluating parameters that is shared by insurance company like height, weight, health, age and smoker or nonsmoker status.
- Organization can guess using staff activity record history of the computing personnel who will be able to quit their job.
- Organization can forecast the likelihood of occurring software error along to year using past experiences and learnings. This knowledge is valid 100 percent on a few software services.

In case of organization knows some risk occurring a lot along one year, organization should save this situation as a numerical data in own list. For this reason, organization can wait a big earthquake with likelihood of 2 percent in own list in every 200 years or three critical errors in Microsoft's IIS (Internet Information Server) to be explored setting likelihood of 1500 percent along the month.

The Cost of Prevention

All in all, organization must determine the cost or expense of protecting of every damage or loss. As an example, organization can calculate the cost of temporary power cut or failure determining "downtime" period that is defined reboot time. But the cost of taking precaution for this issue can be purchasing a UPS (Uninterruptible Power System) system by organization.

Calculated costs which is defined by organization, should be amortized during estimated lifetime of organization's objectives. There can be turn out some credits and secondary costs after reproducing these costs. As an example, setting up fire-suppression mechanism in organization, can cause reducing insurance premiums yearly and it can provide tax advantage in terms of capital amortization. However, that means allocation big part of budget for fire-suppression mechanism, thus organization will not be allocate a budget for other objectives like investment for organization's future, staff training.

3.4 Select Controls for Implementation

The cost-benefit analysis according to previous step is used to decide that controls to perform to compensate likely target organization's purposes. Perhaps, for suggested controls will be necessity a budget, and that budget must be met according to the target organization's budget need. In that step, the last controls to perform depends not only action plan priorities (from the beginning) however on all competing priorities of likely target organization. (Geer, Hoo, & Jaquith, 2003).

Convincing Management

Providing information security in any organization might not be without allocate a budget. In case of the precautions detailed it turns into more costly. Thus, using more costly security systems can be so hard for organization and this process might not always works like that. Information security sometimes can get ahead of "power users" that wants to reach or access organization's critical servers unauthorizedly. A few of "Power users" may be defined politically important users in organization.

Responsible person or team who is work in organization risk analysis need to persuade organization's senior management about how organization should act according to risk analysis outputs after cost-benefit analysis and risk assessment have been done and then organization should be prepared a policy which is officially accepted.

Prioritizing necessary actions and allocating budget for information security are the purpose of cost-benefit analysis and risk assessment. In case of organization's business plan structured provided that not uninsured risk of more than $20,000 during one year, organization can use own risk analysis outputs to identify how much budget need to be

allocated to accomplish their objectives. Besides, risk analysis which is completed by organization may be directory about what they should do in first case then another case and decide which can stay on the desk for assessment in the next year.

Risk analysis is so crucial in terms of determining additional resources for security and it helps to management during approval process. Many directors or managers may not understand or know somethings related to computers. However, cost-benefit and risk analysis are well-known by them. In case of the organization demonstrate $30.000.000 loss of possible threat risk occurred during one year to management adding all forecasted losses and recovery costs and cost of current. Later, it can assist to persuade to senior management to hire more people to work or allocate some budget to obtain more sources.

3.5 Assign Responsibilities

All in all, implementation will depend on staff by the suitable capability. The staff could be ready inside an organization, however for any reasons, likely target organization could settle to delegate accountability to a third party.

3.6 Implementation

In the latest step, the picked necessary controls must be performed by the responsible staff or team at organization. Developing risk mitigation strategies well-known activity for the target organization so crucial. But lots of issues come out throughout implementation. Joining the process third-party individuals while applying successful strategies triggers the issues during implementation. That process makes all implementations process hard and that can create reluctance.

Change management

Change is a concept that we thought as unchanging things. But that is not correct when it comes to security systems. Because too many changes are generally made. This changing can define as software upgrading to the recommended versions, changing firewall policy and rule configurations and probably changing access controls, routing settings on switches. It should need to be so careful to not encounter unwanted and unexpected security issues before changing anything in a system and there must be a available planning to avoid security problems

Change management is generally known a big risk in organizations. That risk is derived from because of recurrence activity is too often, and the conclusion or output of the change might not be as you wish. For this reason, It's too crucial that some changes are paid to the attention of the staff when the change fails. Later, all change transactions may be repeated since beginning.

Ignoring the change management process can subject likely target organization to any possible risks in the future. When necessary changes are being applied, on the change process should need to some monitoring in case of urgency. Later, establishing where the issues happen will be easy by responsible staff. Therefore, we should prepare convenient planning to avoid from possible issues.

Additionally, it is so significant to have action list and policies provide how frequent the changes must be implemented. Some of these actions and policies would grant about the frequency that the changes may be completed, the time period that they may be

influenced, the upgrade patch process to be followed. Besides, the results may not be concluded as expected.

Responsible staff in change management must have the necessary authorizations to effect change in organization. It must not be affected the operation of the organization in terms of cost. For this reason, that process need a bit scaling action during process in case of it is hard to implement change process. For instance, if an organization has never had a policy, it becomes very difficult to implement a change since the organization tends to stick to its cultures. For this reason, to proceed implementing change needs to common understanding and mutual agreement in the organization.

Incident management

Cyber Security incident can be something like a database modify, hack a laptop or also fire may be in target organization. However most important thing in that how to overcome them when incidents happen. Because If we do not take an action about, it may turn into a security matter.

The first stage on incident management is identifying contact right person in the organization or outside the organization. If it is a government organization, related person in organization must need to contact a related agency and notice them regarding to the security breach before incident management team.

Additionally, it is so significant to contact responsible person and have an exchange of ideas in case of occur the incident. If that incident occurs in IT department, the liability can lay on the IT administrators or related to the security staff. If we warn and have an exchange of ideas security guys about incident and then, a solution can be found easily and

we can overcome latest version of the incidents. Related person from incident management team may need to create to overcome incidents contact list which contains experts from inside or outside an organization. For example, specific security incident breaches can need to take an action from forensic experts that can not be available in a IT department. For this reason, the incident can need to help from outside that means third parties.

Alternative management process of security incidence may need to be taking required technical actions for the managing of systems and protection of proofs. Taking like decisions may be pretty hard with the participation a lot of people. For example, if target organization's email server exposes cyber-attack, responsible person may think of cut of organization's internet to get rid of that attack. However, people may not reach their email accounts because of cutting internet with a rule on firewall. For this reason, that needs to have for a perfect ability in order to recreate all the mandatory parts of argument or evidence list provided that the business activities of all organization staff.

Besides, it is too crucial to identify which documents will be reported and what defined in the documents. Cyber security breaches may be too significant for the next case. When responsible person asks to investigate incident history to what can have the reason of the security incidence. These reports may be so crucial to track unauthorized access attempts when we ask to judge the person that is responsible for all breach and for this reason, the incident must have own case record history. Incident documentation reports should not be just consist of writing, However it should contain pictures and videos in order to support evidence.

User rights and permissions reviews

It is so significant determining user rights, authorization and permission controls while overcome the issues of sensitive data change, loss, modify and breach. That means the organization's sensitive data breach is originated from lack of determining user rights, authorization and permissions correctly. End users can be restricted by authorization. However, authorization levels may happen unauthorized access to sensitive data because of manipulation of their user account credentials. It is so crucial checking of user permissions regarding to administrator access or guest access because of differences log in credential information. Guest user permission should log in system as guest and administrator users with the admin rights should log in the same way.

Periodically checking of the end user rights, authorization and permissions so important in order to prevent actions of cyber-attackers. To prevent unauthorized access, all information like user credentials, organization's sensitive data must be encrypted with a code and only authorized people should access the data by defined user rights permissions.

Perform routine audits

Information security audits are so crucial when the security breach an occurs and audit's output will help to understand what is happening on background. It will prove us how much double checking is so significant in information security policy. Sometimes, the organizations may need to check whether their network secure and all is working properly or not. That will cause to transfer us to contact with third part companies that is responsible

for external audit process. Thus, organizations update their rights and permissions as they want according to latest policies.

The organizations are responsible of keeping pace with routine in a short time when it is considered to change all busines process because of rapid change. Organizations, especially in security issues must have enough time to understand what is going on and they spent their time to understanding of security matters.

Information security audits can be considered part of log analysis tool. Required action plans may be defined with this information. For example, unauthorized administrator access can occur in a range of time. For this reason, knowing the automatically defined likely undesirable activities in a system so crucial for the organization.

The types of auditing need to be considered by organizations. First type of auditing is privilege account management. This type of auditing is helped to identify necessary permissions and user rights when someone is tried the access organization's sensitive data. At the same time, it provides to configured correctly different administrator's accounts permissions on organization's network.

Second type of audit is resources usage auditing. This type of audit is used to understand if the resources in the organization are using properly by staff. According to this auditing, organization can identify necessary policies and actions on system, network, database, and applications to prevent unauthorized access.

The third type of auditing is escalation audit. In case of disaster recovery, escalation auditing outputs help the organization to prevent unexpected issues. The output of this

auditing process can be used to identify or guiding to organization if the organization own the latest technology or necessary equipment in order to handle disaster.

The last type of audit is administrative auditing. That auditing process is in charge of identify if the organization is recording entire the material or items in their system which needs to be documented. For this reason, organizations need to collect and record documented information in lights of audits to take quick action when the problem has been occurred.

Enforce policies and procedures to prevent data loss or theft

Implementing risk mitigation procedures on organization is so important thing in term of preventing to loss of sensitive data and organization's resources. In terms of physical policy, performing basic physical policies on organization can prevent easily sensitive data loss. Organizations absolutely must have own policies and procedures to access sensitive data or information. For example, Organizations may implement some visitor procedures like visitor card or recording visitor credentials in order to provide safe visit conditions. Besides, a security escort can come along with visitor or guest during visit.

In terms of database, implementing well known data policies may be so hard to perform on organization. It means that sensitive data belong to organization can be store on end user' laptop or external storages like USB, hard disk.

Advanced protection policies and procedures can prevent all sensitive data breach and loss in internal and external. Focusing only one case may be unsecure action in terms of the cyber-threats. For this reason, organizations should determine and implement data

or information access policies and procedures for everyone not only for specific group or trustable people.

Undesired activities like storing insecurely big data on our network and system may cause sensitive data breach and loss. For this reason, Well-known and most available policies and procedures should always be updated to prevent illegal access from internal network and external network.

Enforce technology controls

Performing technology controls periodically in organizations can be another alternative for risk mitigation. So, technological controls in terms of risk should be done before latest technology implemented like new software, cloud computing, IoT, AI (artificial intelligence) or Blockchain. In the implementation process, IT is responsible for the new software installation on server and should make sure that all is working properly after implementation process. Besides, IT should check whether the software is a malicious software or not for organization's security system.

Moreover, organizations should not be forgotten that, high technology solutions contain some errors because of developed by human hand. For this reason, the implementation process must be monitored step by step in organizations.

Data Loss Prevention (DLP)

Organizations may enable Data Loss Prevention feature determining necessary policies and rules on network to prevent and control data transfer or loss against undesired data issues. Organizations should determine some circumstances and hardened policies on data that is sensitive for organization before takes an action on a specific data. For this reason, organization's security infrastructure should be appropriated in terms of policy and strategy because of data loss generally cyber-security breaches.

Actually, that is well known it is so hard to implementing risk mitigation strategies and hardened data loss prevention policies and some specific procedures and collecting evidence by cyber-security experts. Organizations must monitor process step by step to performing to latest procedures and policies and strategies perfectly in order to protect sensitive data. Performing data loss prevention process in organizations must not be completed by one person that is responsible. It should be determined with agreed common decisions by every staff who is work in organization. Because, that process services to everyone in organization.

4. EFFECTIVENESS EVALUATION

Measuring and verifying of organization's risk mitigation objectives have been meet can be defined as Effectiveness assessment. Although risk mitigation and risk assessment are completed in organization at different time, the effectiveness evaluation process must be performed continual. There are two reasons of this process in the risk management.

First reason, risk evaluation is not a certain science to clarify everything. There are uncertainties connected to expected threat frequency, impact of possible threats, probability of threats and the real range of threats. Besides, there are some uncertainties in the forecast of benefits and costs for each control option. The uncertainties can cause of misunderstanding and misinterpreting in the risk mitigation action plan. For this reason, risk mitigation plan should be evaluated in terms of risk mitigation plan success or failure. Risk evaluation maintains helpful feedback to in terms of providing accuracy to the process.

Second reason, the organization's infrastructure might not be kept static. An organization's priorities, policies, personnel, software, computers, and network are going to modified with time. Risk mitigation or risk assessment operation must be performed continual or kept up to date with latest information.

5. CONCLUSIONS

In conclusion, we explained the information security risk management process and relationship between parameters step by step. Besides, we defined most used methodologies for ISM and approaches for risk analysis. In the case study risk assessment process, the five assets have been defined for organization such as staffs, RMS (Revenue Management Systems) software, reputation, electronic data, and IT hardware. The organization assets that are exposed by cyber-threats are affected following data breaches or theft, cross-site scripting, man in the middle attack, DDOS, DOS, SQL injections, social engineering, fraud, email phishing, password broken, human error and power failure. To identify vulnerabilities on organization assets is being used industry standard technical, physical, and administrative controls. These controls are used to prevent breaches identified vulnerabilities in assets as well.

The restriction of this study is number of organization assets used. It is so hard to find an organization that have just five assets. Responsible team from ISM (Information Security Management) should work with stakeholders to find and determine true information and vulnerabilities for whole organization assets. On the other hand, responsible person should update processes and follow methodically while preparing management report from this study results. The guidelines that are used in this study are valid for whole industry sectors too without selection of organization.

Qualitative method is being used to assess the identified risks on organization. Moreover, organizations usually give priority quantitative approaches using some difficult parameters like dollars, euros. To identify risk management issues following phrases is being widely used such as total cost of ownership, exposure factors, the annual rate of occurrences, single

loss expectancy and annualized loss expectancy. Return on Investment calculations and the Total Cost of Ownership, while putting together with Risk Analysis must consider appropriate budgeting.

REFERENCES

Alberts, C., and Dorofee, A. (2002). *Managing information security risks: the OCTAVE approach*. Reading, MA: Addison Wesley.

Blakley, B., McDermott, E., and Geer, D. (2002). Information security is information risk management. In proc. of *ACM Workshop on New Security Paradigms (NSPW'01)*, 97-104.

Decker, R. (2001). *Key elements of a risk management approach*. GAO-02-150T, U.S. General Accounting Office.

Farahmand, F., Navathe, S., Sharp, G., and Enslow, P. (2003). Managing vulnerabilities of information systems to security incidents. In proc. of *ACM 2nd International Conf. on Entertainment Computing (ICEC 2003)*, 348-354.

Geer, D., Hoo, K., and Jaquith, A. (2003). *Information security: why the future belongs to the quants*. *IEEE Security and Privacy*, 1(4), 24-32.

G. Stoneburner, A. Goguen and A. Feringa, "*Risk Management Guide for Information Technology Systems*," NIST Publication 800-30, 2002.

ISO/IEC:13335, *Information technology — Security techniques — Management of information and communications technology security*, 2004.

ISO/IEC, Guide 73:2002 *Risk Management Vocabulary Guidelines for use in standards*, 2002.

C. Mike, S. David, M., James and G. Darril, (ISC)2 *CISSP certified information systems security professional official study guide*, 8E & CISSP official (ISC)2 practice tests, 2E., Indianapolis Sybex, 2018.

ISO:31000, *Risk management* — Guidelines, BSI Standards Publication, 2018.

W. Michael and M. Herbert, *Management of Information Security*. 3rd ed., Course Technology. Cengage Learning, 2010.

C. P. Pfleeger and S. L. Pfleeger, *Analyzing Computer Security*, Michigan: Prentice hall., 2011.

W. Evan, *Security Risk Management*, Waltham: Syngress, 2011.

F. T. Harold and K. Micki, *Information Security Management Handbook*, Auerbach Publications, 2007.

Gordon, L, and Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5, 438-457.

Hoo, K. S. (2000). *How much is enough? A risk management approach to computer security*. Retrieved October 25, 2006, from http://iisdb.stanford.edu/pubs/11900/soohoo.pdf.

McClure, S., Scambray, J., and Kurtz, G. (2001). *Hacking Exposed: Network Security Secrets and Solutions*, 3rd ed. New York, NY: Osborne/McGraw-Hill.

Mercuri, R. (2003). Analyzing security costs. *Communications of the ACM*, 46, 15-18.

Microsoft. (2004). *The security risk management guide*. Retrieved October 25, 2006, from http://www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/default.mspx.

National Bureau of Standards. (1975). *Guidelines for Automatic Data Processing Risk Analysis*. FIPS PUB 65, U.S. General Printing Office.

National Institute of Standards and Technology. (2002). *Risk Management Guide for Information Technology Systems*, special publication 800-30.

National Institute of Standards and Technology. (2003). *Guideline on Network Security Testing*, special publication 800-42.

Peltier, T. (2005). *Information Security Risk Analysis*, 2nd ed. New York, NY: Auerbach Publications.

Shon, H. (2013). CISSP All-in-One Exam Guide, *Risk Management, Risk Assessment and Analysis*, pp. 70-100.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York, NY: John Wiley & Sons.

Vorster, A., and Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. In proc. of *ACM Annual Research Conf. of the South African Institute of Computer Scientists and Information Technologists (SAICSIT 2005)*, 95-103.

Enisa Risk Management, Risk Assessment Inventory (2006) *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools* 2006, 5-6

APPENDIX A: Key Terms

- **Accountability:** the assignment of responsibilities and traceability of actions to all involved parties.
- **Availability:** the maintenance of dependable access of users to authorized information, particularly in light of attacks such as denial of service against information systems.
- **Confidentiality:** the protection of information against theft and eavesdropping. Integrity: the protection of information against unauthorized modification and masquerade.
- **Risk assessment:** the process to understand the value of assets, system vulnerabilities, possible threats, threat likelihoods, and expected impacts.
- **Quantitative risk analysis** Assigning monetary and numeric values to all the data elements of a risk assessment.
- **Qualitative risk analysis** Opinion-based method of analyzing risk with the use of scenarios and ratings.
- **Risk management:** an organization's or company risk assessment and risk mitigation.
- **Risk mitigation:** the process to strategically invest limited resources to change unacceptable risks into acceptable ones.
- **Threat:** the potential for some damage or trouble to an organization's information technology environment.
- **Vulnerability:** a weakness or flaw in an organization's system that might be exploited to compromise security.
- **NIST 800-30 Risk Management Guide for Information Technology Systems** a U.S. federal standard that is focused on IT risks.
- **Facilitated Risk Analysis Process (FRAP)** A focused, qualitative approach that carries out prescreening to save time and money.
- **Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)** Team-oriented approach that assesses organizational and IT risks through facilitated workshops.

- **AS/NZS 4360** Australia and New Zealand business risk management assessment approach.

- **ISO/IEC 27005** International standard for the implementation of a risk management program that integrates into an information security management system (ISMS).

- **Failure Modes and Effect Analysis** Approach that dissects a component into its basic functions to identify flaws and those flaws' effects.

- **CRAMM** Central Computing and Telecommunications Agency Risk Analysis and Management Method.