TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Cyber Security Engineering

Fuad Budagov 184055IVSB

Information Technology Risk Assessment of the Indoor Advertising Platform AdZillah

Bachelor's Thesis

Supervisor: Mohammad Tariq Meeran (PhD)

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Küberturbe tehnoloogiad

Fuad Budagov 184055IVSB

Sisereklaamiplatvormi AdZillah infotehnoloogiline riskianalüüs

Bakalaureusetöö

Juhendaja: Mohammad Tariq Meeran (PhD)

Tallinn 2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Fuad Budagov

17/05/2021

Abstract

Nowadays, many startup companies do not prioritize security in the first place. However, the majority of them deal with sensitive data of customers. Over time, the importance of information is increasing, it also increases a data breach risk which can result in failure to comply with information security standards and eventually lead to loss of business. Security breach cannot only harm those companies but also ordinary people who are not even aware of risks and relied on those companies.

Information technologies risk assessment is important to an organization for understanding risk exposure of confidentiality, integrity, and availability of IT assets.

In this research author presents a comprehensive mapping report on risk assessment for information systems. The research was performed by the author using several methods to gather required data from the company AdZillah.

The outcome of this research can be used by small enterprises to reduce security risks identified through risk assessment approach and to strengthen the company's IT security in all levels. In addition, it helps an enterprise to conduct cyber security risk analysis regarding exploration of security breaches.

The thesis is in English and contains 35 pages of text**,** 6 chapters, 9 figures and 19 tables.

List of abbreviations and terms

Ad	Advertisement
AP	Access Point
AWS	Amazon Web Services
BYOD	Bring your own device
CBA	Cost benefit analysis
CEO	Chief executive officer
CMO	Chief marketing officer
DRP	Disaster Recovery Plan
e.g.	Exempli gratia (for example)
etc.	Et cetera (and other similar things)
HP	Hewlett-Packard
ID	Identity document
IPsec	Internet Protocol Security
IR	Incident Response
IT	Information Technology
NDA	Non-disclosure agreement
n/a	Not applicable
OÜ	Osaühing (Private limited company)
PhD	Doctor of Philosophy
RAID	Redundant Array of Independent Disks
SecSDLC	Secure software development life cycle
SSH	Secure Shell
US	United States
VPN	Virtual private network
WC	Water closet
WEB	World Wide Web
Wi-Fi	Wireless Fidelity

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Motivation

Information technology (IT) solution are actively being used in various critical sectors, the protection of IT systems becomes highly relevant. In one of his speeches, famous US government official, Richard Clarke said “If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked”. [1] I do not necessarily agree with the idea that companies spending more on coffee deserve to be hacked. In fact, many IT specialists consume significant amount of coffee while performing their jobs. But I fully support the belief that businesses should spare enough funds to protect their IT security.

Currently, many businesses and government agencies are actively using information systems to perform their work. Information can be expressed in many forms, on paper, electronically, or verbally. Regardless of the form of information, it must be protected in an appropriate manner. Information security can be ensured by ensuring the confidentiality, integrity and availability of information at the appropriate level. Failure of any of the above three elements can be considered as a failure of the information security implementation. [2]

1.2 Research problem

Employees of AdZillah use their personal electronic devices which includes personally owned cellphones, smartphones, tablets, laptops and computers for work purposes, and that can pose a risk from a security point of view.

AdZillah has a visible Internet profile, has a relevant size, and handles sensitive information. In addition, employee personal information, strategic plans, products, services, market plans, customer information, and suppliers are stored digitally at AdZillah systems.

Company’s IT systems have been outsourced to the third-party, which provides services for the web development and testing.

Company information, such as customer data or emails, is accessible from employee private smart phones, tablets, and personal computers.

As a result, AdZillah, as any other business, can be exposed to cybercrime due to mentioned elements above.

1.3 Research goal and objective

The aim of this research is

- To identify and manage potential problems in data security that could affect IT infrastructure of the company and put AdZillah's customers at risk
- To perform enterprise cyber security risk analysis according to identified vulnerabilities of the company's IT system.

Objectives of the research are:

- To conduct gap analysis between the acceptable standards, regulations and the company current state
- To propose risk management approach
- To conduct risk analysis

1.4 Research questions

This research will cover answers to following questions:

- What are the potential IT related risks at AdZillah?
- How can identified risks at AdZillah be evaluated through the risk assessment process?

2 Theoretical background

2.1 Risk management

In this chapter, we will describe the characteristic of risk management components and how risk assessment can be performed and followed up.

Risk management is a process for any organization of identifying potential risks associated with information assets of a business and achieving goal by taking required security measures to reduce the identified risks. Well-structured risk management practices are the duty of general management of an organization in order to reduce risks to an acceptable level while keeping the cost of security solutions at its minimum level. [3]

Risk management is combination of risk identification, risk assessment and risk control which is shown in Figure 1.

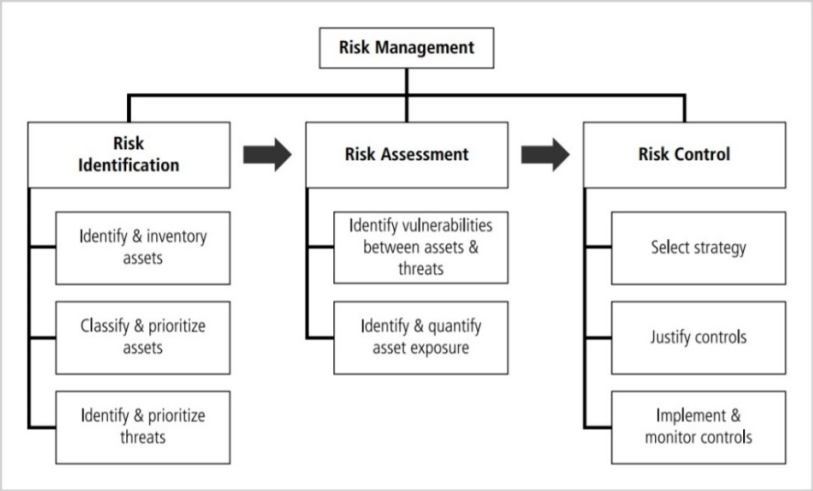

Figure 1. Components of Risk Management (Source: [3])

It is important to understand definitions of 3 concepts asset, threat, and vulnerability in risk management.

Information assets can be databases, software code, etc., in general, anything that are valuable for IT system or organization. Threat is a danger to an asset. Exploitation is to use a vulnerability to cause damage or harm to IT system. Vulnerability is a weakness or gap in a system that can be exploited by a threat actor. [4]

2.2 Risk identification

To begin the process, risks must be identified, classified, and prioritized in terms of its probability in order to make an assessment and decision. Process of threat assessment identifies the risks each asset takes, after organizational assets have been identified.

The components of risk identification are illustrated in Figure 2. [3]

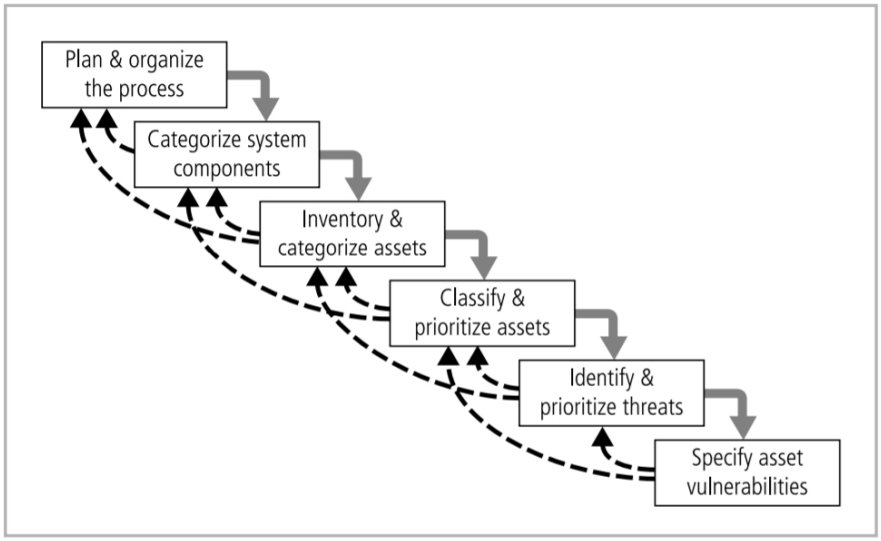

Figure 2. Components of Risk Identification (Source: [3])

2.3 Risk assessment

Risk assessment is the process of combining risk identification, risk analysis, and risk evaluation. It is part of risk management which evaluates threats and vulnerabilities once, they have been identified in information assets of an organization. Each asset is given a risk rating during the risk assessment process. This rating has no absolute explanation. It is helpful in determining risks related to each vulnerable system and to improve risk scores. [3]

There are several core steps for performing and documenting a risk assessment for small to mid-sized companies.

2.3.1 Risk determination

Risk determination process is the assessment of consequences and incident likelihood to determine risk level. [4]

Likelihood is the probability that an attacker would take benefit of a vulnerability. A number is assigned to likelihood in a risk assessment. Risk rating is the result of multiplying likelihood by impact. [4] Risk rating matrix is described in Figure 3 below:

Risk rating = likelihood x impact *(Source: [4])*

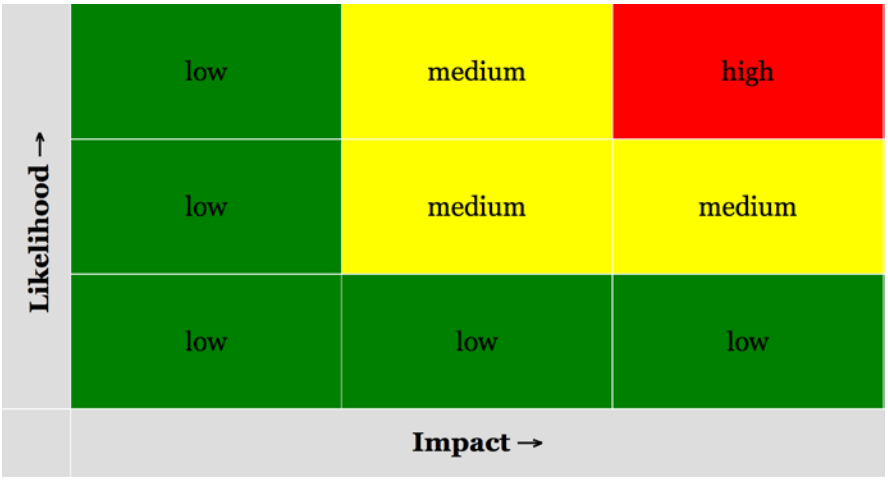

Figure 3. Risk Rating Matrix (Source: [5])

2.3.2 Identification of possible controls

The main goal of the risk assessment is to control risks after determining each vulnerability and its associated threat, and eliminate them as much as possible, however, it is impossible entirely. Therefore, there will always be some remaining risks in a certain level. You must create a list of possible controls to threats and each of their vulnerabilities that contain residual risk. Residual risk is the amount of risk or danger to the information asset which remains even after risk is reduced by implementing controls. It is illustrated in Figure 4 below:

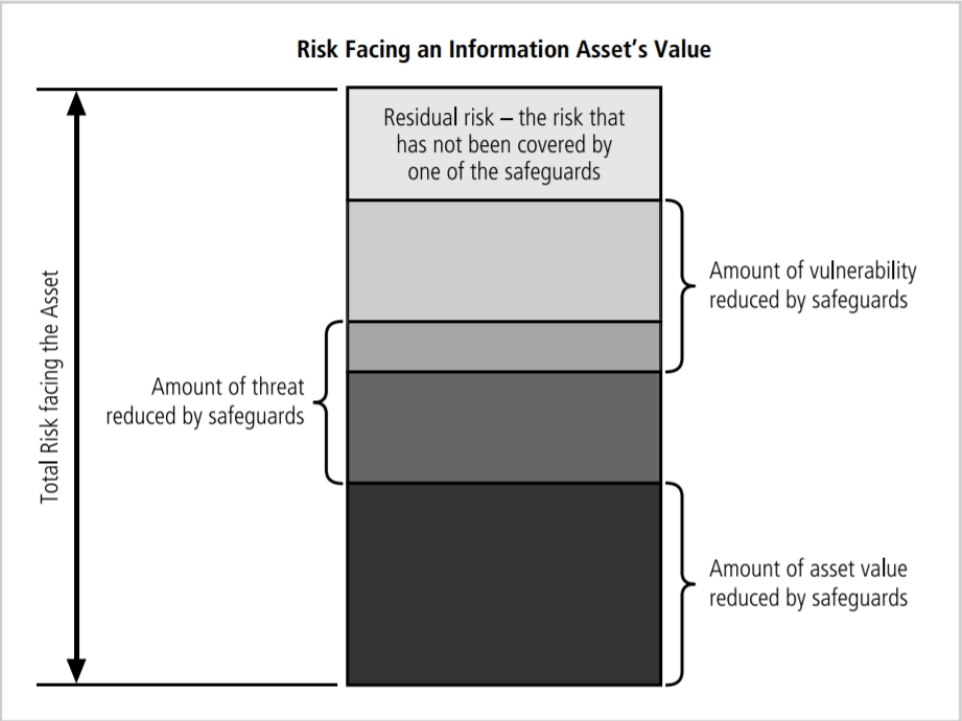

Figure 4. Residual Risk (Source: [3])

There are 3 types of risk controls: policies, programs and technologies.

Policies are set of rules indicates organization way to security.

Programs are activities such as education, training or awareness of employees for those using the computer and network resources of the company and that are mentioned in the security policy. Program security policy is illustrated in Figure 5.

Finally, technologies are technical implementation of policies to handle risks when they will occur. There are various technologies used in implementation of policies such as firewall, VPN, cryptography, intrusion detection and preventions systems and security tools. [3]

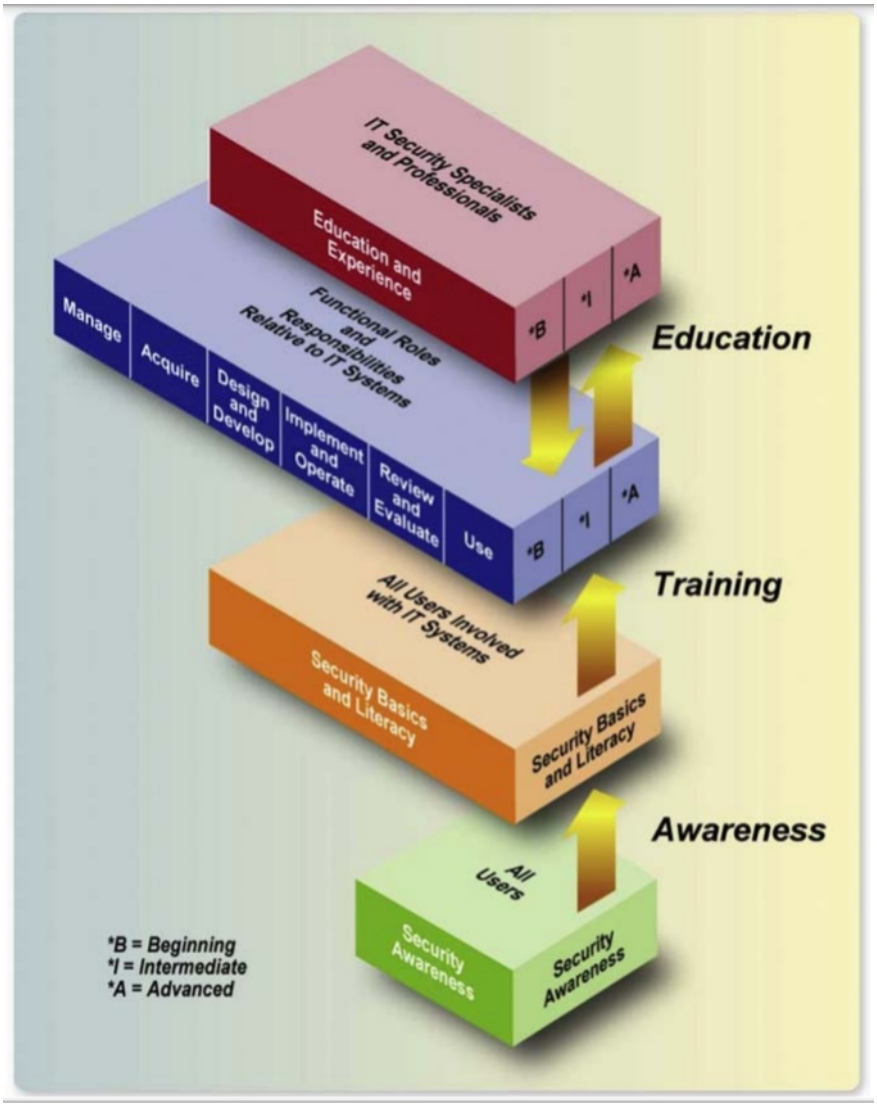

Figure 5. Program Security Policy Overview (Source: [4])

2.3.3 Documenting risk assessment

Once the risk assessment has been completed, we will have a list of information assets with details. A well-structured matrix or worksheet contains data gathered in previous steps will help to systemize risk assessment results. Risk assessment matrix is the initial document for the next step – control strategy. [3]

2.4 Risk control

Risk control strategy is the last step in risk management. Once, risks have been determined through the risk assessment, information security officials are informed to control risks. As it is described in Figure 6 below, risk control strategies are transfer, mitigate, accept and terminate strategies. [3]

Figure 6. Risk Control Strategies (Source: [6])

2.4.1 Risk mitigation

Risk mitigation strategy purpose is to minimize impact of risks recommended from the risk assessment process. There are 3 types of plans to implement risk mitigation:

Incident response plan is a set of procedures to detect and mitigate unexpected event before or while an incident is in progress.

Disaster recovery plan is the most common mitigation plan used to recover loss from any disaster or incident. [3] Small to mid-size businesses may incorporate it as part of business continuity plan as well. [7]

Business continuity plan is the most strategic plan which provides continuation of a business in case of a natural disaster by ensuring running of IT system of an organization. [3] It provides non-top running of IT system in midst of the crisis; however, disaster recovery plan is focused to recover IT system to full functionality after disaster occurs. [3]

2.5 Conclusion

In summary, risk management is very important for any business whether it contains risks or no risks. To achieve an effective risk management, an organization need to follow all steps: risk identification, risk assessment and risk control strategies.

Regular communication and mutual cooperation of executive managers and IT professionals will help to build a successful risk management.

Having a good risk management, one can anticipate any risks that may have a negative impact on a business.

Well-structured risk management enables to see risks, measure the impact on the business if the risk occurs, prioritize which risks must be taken into account first and foremost, and then take the necessary measures to reduce the risks.

3 Methodology

This chapter describes the methods used to collect and analyze the data.

3.1 Research method

Scientific research methods are divided into two categories: quantitative and qualitative.

Quantitative research focusses on numerical aspects and graphs. It makes it possible to conduct statistical analysis using data, which gives preference to the comparison of different data sets and the generalization of results. Common quantitative methods are surveys, number-based observations and experiments.

In contrast, qualitative research uses mainly word-based information. It is effective in understanding of concepts, thoughts, or experiences. Common qualitative methods are word-based observations, interviews and literature reviews. [8]

This research has been conducted using a qualitative method to gather and analyze the research data.

3.2 Data collection

In this work, the data is collected through on-site interviews with CEO and IT specialist of the company, and on-site visit to company to observe and collect data regarding the physical and environmental safeguards of the IT system and its operational security to perform risk assessment. [10] Books, scientific articles and previous research have also been reviewed to collect necessary data, as well as comparative analysis has been conducted.

3.3 Risk assessment method

Qualitative type of risk assessment has been conducted, and risk rating is defined as low, medium and high. Risk assessment template is referenced from Information Technology Risk Management Guideline of Virginia Information Technologies Agency.

4 Analysis and result

4.1 Introduction to risk assessment

Author performed risk assessment for Indoor Advertising Platform AdZillah's IT system to identify risks and prepare risk assessment matrix to reduce risks of the company. No risk assessment has been done since the company was established.

Qualitative risk assessment method which is described in Chapter 3.3 was used to perform risk assessment to identify:

- Vulnerabilities
- Threats
- Risks
- Risk Likelihoods
- Risk Impacts

The following people were involved in this risk assessment and their roles are described as:

- Fuad Budagov, Cyber Security Engineering student at TalTech, prepared and conducted risk assessment;
- CEO, reviewed the risk assessment report prior to completion, provided information through interview;
- IT specialist, provided information through interviews.

Risk classification is defined in Table 1.

Table 1. Risk Level Classification

Level of Risk	Description of Risk
Low	Low risk is acceptable and unlikely cause to accidents, but it must be monitored to discover changes that does not escalate to a higher level.
Medium	Medium risk can be acceptable, however, the risk must be observed regularly to bring it as low as possible level.
High	High risk is not acceptable which may have severe or catastrophic result on organization's IT System.

4.2 IT system characterization

4.2.1 Company overview

Established in 2019, AdZillah company is one of the fresh startup IT companies in Tallinn, Estonia providing indoor and outdoor advertisement services. AdZillah mission is to use technological solutions and the state art of technology in order to create an easy way to run banner ads indoor and outdoor. Company is located in Tallinn, Estonia.

The company rents the half of the 2nd floor of a building, which has been set up with four full equipped rooms. In each room, different department employees perform their daily work.

In addition to that, the company has a server room, meeting room, storage, kitchen, WC, waiting area and a reception area with printer. A secretary takes care of phone calls, and greets the customers.

The company does not have a large management structure. Therefore, they just have a CEO who is responsible for general management, business and technical, for AI and hardware components of idea, and CMO who is responsible for project and business development, promoting the business. Furthermore, there is an IT specialist to monitor and maintain the computer systems and networks of AdZillah, and a digital law specialist to trademark registration and patenting of idea related technologies. Lastly, the reception employee handles email queries and phone calls, greet visitors and performs other administrative duties. Office layout is shown in Figure 7.

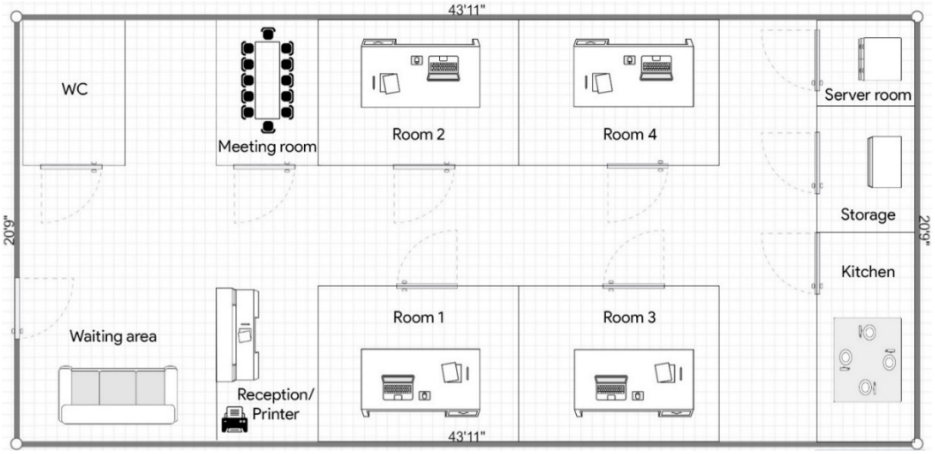

Figure 7. AdZillah Office Layout (Source: Author created)

4.2.2 IT infrastructure characterization

The company has its own server room with proper locks and ventilation. However, the temperature is approximately above 30 degrees Celsius on average.

There are several networking devices such as switches, routers, a firewall in the server room.

The computer system and the network are administered by an IT specialist; however, its web development and testing are performed by an outsource partner.

All company employees connect to the central server with laptops that run as thin clients. Each employee has one laptop. They are allowed to take it home or use it as a personal computer.

Information flow diagram is illustrated in Figure 8.

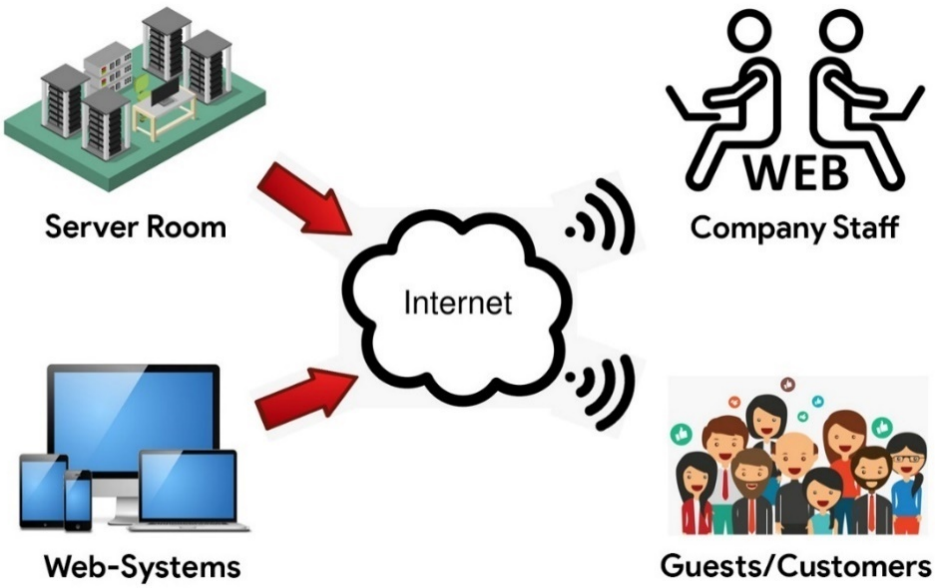

Figure 8. AdZillah Information Flow Diagram (Source: Author created)

The company stores customers' data in the central system via an internal web application. The employees can also connect to the servers remotely from external locations to access the web application. This usually happens when the staff works from home or while traveling.

RAID system is not configured in the central server where company's critical data is stored.

Regarding email, the company has an email server located at the partner's datacenter. The email is downloaded to the employee laptops via the internet, and it gets scanned for viruses

and spam. Email messages may contain confidential data about customers, and according to their IT agreement, the partner could potentially have access to this information.

Lastly, there is a guest wireless network for guests or customers in the waiting area.

Figure 9 describes network map of the company.

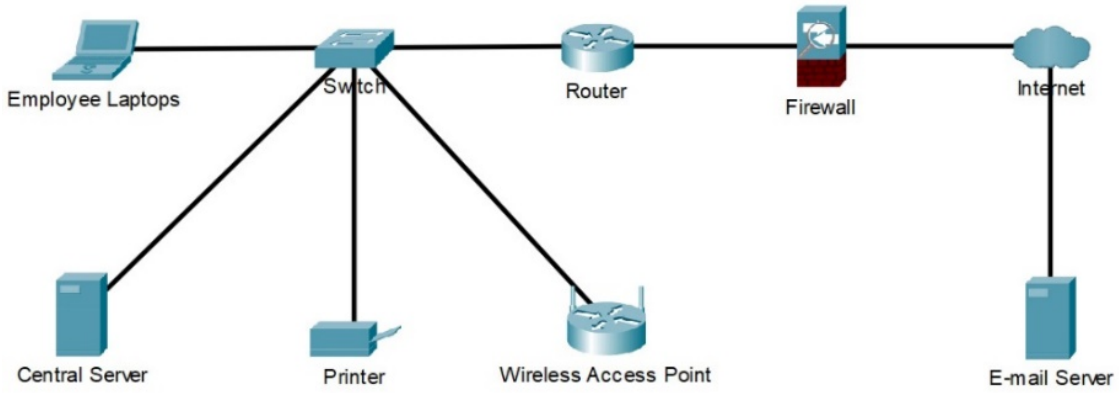

Figure 9. AdZillah IT System Boundary Diagram (Source: Author created)

Table 2 describes IT system identification and ownership:

Table 2. Identification and Ownership of AdZillah IT System

IT System Name	AdZillah IT System		
Owned By	AdZillah OÜ		
Physical Location	AdZillah J. Koleri 26/2, Tallinn		
Business Service Industry	Providing indoor and outdoor advertisement services		
Owner of System	CEO	**System Administrator**	IT Specialist
Owner of Data	CEO	**Data Custodian**	IT Specialist
Other Information	AdZillah OU has been operating since 2019		

IT system assets are described in Table 3:

Table 3. IT System Assets

IT System Components	SecSDLC	Risk Management System Components
People	Employee Non-employee	CEO, CMO, IT Specialist, Digital Law Specialist, Receptionist Web developer and Tester at outsource partner, customers, visitors
Hardware	System devices and peripherals, networking devices	Laptops, server, printer, router, switch, firewall, wireless AP
Data	Information	Personnel data, customer data, financial data

IT system users are illustrated in Table 4 below:

Table 4. IT System Users

Position	Employee ID	Security clearance level	Role
CEO	1	High	general management, business and technical
CMO	2	Medium	project and business development, promoting the business
IT Specialist	3	High	monitor, maintain and troubleshoot the computer systems and networks
Digital Law Specialist	4	Low	trademark registration and patenting of idea related technologies
Receptionist	5	Low	handles email queries and phone calls, greet visitors and other administrative duties

IT system hardware is described in Table 5 below:

Table 5. IT System Hardware

Assets	Manufacturer	Model	Physical location	Logical location	Controlling entity
Employee laptops	HP	n/a	Rooms	n/a	Employee
Router	Cisco	n/a	Server room	n/a	IT Specialist
Switch	Cisco	n/a	Server room	n/a	IT Specialist
Firewall	Cisco	n/a	Server room	n/a	IT Specialist
Wireless Access Point	Cisco	n/a	Reception	n/a	IT Specialist
Server	HP	n/a	Server room	n/a	IT Specialist
Printer	HP	n/a	Reception	n/a	Receptionist

IT system data and sensitivity are indicated in Table 6:

Table 6. IT System Data and Sensitivity

Type of Data	Sensitivity Ratings		
	Confidentiality	Integrity	Availability
Personnel Data	**Low** Employee data does not contain any sensitive information; therefore, it is public	**Medium** It is stored in central server	**Low** Not daily used
Company Financial Data	**High** Data is private	**Medium** It is stored in central server	**Medium** Regularly updated
Customer Data	**High** It contains customers' private information such as photos (if available)	**Low** Currently, it is low; no customer data is stored in database **High** In future, it will be high; when customer data will be stored in database	**Medium** Planned to be updated regularly
Email Data	**High** It contains company private information	**High** It is stored in a partner center	**High** It is used daily

4.3 Identification of Risks

Risks are listed according to pairing vulnerabilities identified and described in chapters 1.2 and 4.2.2 and threats.

4.3.1 Vulnerability identification

Table 7 shows vulnerabilities which are identified by:

- Interviews with AdZillah's CEO and IT Specialist
- On-site visit to company

Table 7. Identified vulnerabilities

№	Vulnerability	Threat source	Impact
1	Temperature in the server room	Environment	Fire can occur in server room
2	Fire and anti-theft alarm	Environment Insider	Can cause fire incident and devices from being stolen
3	Internal network security	Unauthorized users	Connecting guest network to the switch that central server is also connected, may grant unauthorized access
4	VPN security	Unauthorized users	Not using a secure remote access VPN increases confidentiality and unauthorized access risks
5	Password strength	Unauthorized users	Passwords the users use can be weak, moreover, guest network and central server is connected to the same switch
6	Email server	Industrial espionage	It is located at the partner's datacenter, outside of the company
7	IT Outsourcing agreement	Industrial espionage	NDA is not signed between parties in addition to general agreement to guarantee data confidentiality
8	BYOD policy	Insiders	Not having a BYOD policy to add personally owned devices to BYOD program for monitoring increases company security risks

9	Data redundancy	Hacker Environment	Not having configured RAID technology in the server increases all data loss in case of hard drive failure Temperature in server room can reduce server running efficiency, or device failure
10	Disaster recovery plan	Nature	There are not procedures to provide non-stop working operation in case of disaster

4.3.2 Threat identification

Threats are identified by:

- Interviews with AdZillah's CEO and IT Specialist
- On-site visit to company

Identified threats are listed in Table 8 below:

Table 8. Identified threats

Threat	Threat source	Motivation
Malicious use	Hacker	Curiosity, ego, intelligence, revenge
Unauthorized access or use	Unauthorized user	Challenge, ego, rebellion
Theft of equipment	Insiders	Competitive advantage
Data theft	Industrial espionage	Competitive advantage Economic espionage
Computer crime	Computer criminal	Monetary gain Unauthorized data alteration
Hardware failure	Environment	Hardware can fail and stop the services it provides
Fire	Environment	Company to catch on fire
Disaster	Nature	Nature event

4.3.3 Risk identification

Risks are identified according to combination of vulnerabilities and threats. Table 9 indicates identified vulnerabilities:

Table 9. Identified Risks

Risk №	Vulnerability	Threat	Risk of Compromise of	Risk Summary
1	**Temperature in the server room** is above 30 degrees Celsius	Fire Hardware failure	Availability of AdZillah IT System and data	The server room is running hot and there is a lot of expensive devices in the company included server room devices that can catch on fire.
2	**Fire and anti-theft alarm** are not installed	Fire Theft of equipment	Availability of AdZillah IT System and data	Can cause serious hazards to human life There is a risk of theft in company not having an installed anti-theft alarm
3	**Internal network security**. Wireless router for guests or customers is connected directly to the switch which is central server also connected	Unauthorized access or use	Confidentiality and Integrity of AdZillah IT System data	Having unauthorized access to the central server and AdZillah IT System
4	**VPN security**	Unauthorized access or use	Confidentiality and Integrity of AdZillah IT System data	Not using a secure remote access VPN increases confidentiality and unauthorized access risks
5	**Password strength** is required	Unauthorized access or use	Confidentiality and Integrity of AdZillah IT System data	Passwords the users use to access internal web-system can be weak and it increases risk of unauthorized access

6	**Email server** is located at the partner's datacenter	Industrial espionage	Confidentiality and Integrity of AdZillah IT System data	Having access of partner to emails which can contain confidential data of company included customers' data
7	**IT Outsourcing agreement**	Industrial espionage	Confidentiality and Integrity of AdZillah IT System data	NDA is not signed between parties in addition to general agreement to guarantee data confidentiality
8	**BYOD policy**	Theft of equipment	Confidentiality and Integrity of AdZillah IT System data	Not having a BYOD policy to add personally owned devices to BYOD program to monitor increases company security risks
9	**Data redundancy**	Fire Unauthorized access or use	Confidentiality and Integrity of AdZillah IT System data	Not having configured RAID technology in the server increases all data loss in case of hard drive failure Temperature in server room can reduce server running efficiency, or device failure
10	**Disaster recovery plan** is not prepared	Natural disaster	Availability of AdZillah IT System and data	There are not procedures to provide non-stop working operation in case of disaster

4.4 Analysis of Risk Controls

The aim of control analysis is to make a list of safeguards or countermeasures for the AdZillah's IT System. Prepared safeguards are security controls which are listed in Table 10 below:

Table 10. Security Controls

Control Area	Description of Controls
1 Risk Assessment	Requires implementation of risk assessment in each 3 years control risks and avoiding from an unexpected serious threat
2 IT Disaster Recovery Planning	Requires preparation a disaster recovery plan to recover continuity of operations within 48 hours minimize financial loss and keep operability
3 IT System & Data Backup & Restoration	Requires using RAID 5 level in central server to backup data
4 Password Management	Requires using a complex password not less than 8 characters, combination of letters and numbers, at least 1 upper case & 1 lower case letters, 1 number and 1 special character by Windows Active Directory
5 Remote Access	Requires configuration a remote access IPsec VPN in Cisco ASA firewall allows users secure connection from distance
6 Encryption	Requires encryption of passwords during transmission and encrypt data through SSH to provide transmission securely
7 Facilities Security	Requires secure card-key access system not to allow unauthorized person to get access private areas, it also requires fire and anti-theft alarm to prevent theft actions, and lastly, it requires air conditioner at the server room to reduce temperature and to ensure efficient running of devices at the server room
8 Access Determination & Control	Requires removal of both physical and logical access to company in case of termination employee
9 IT Security Awareness & Training	Requires activities such as education, trainings or awareness of employees for those using IT System of company
10 Acceptable Use	Requires NDA agreement with partners to keep AdZillah’s confidential data as trade secret and promises not to disclose
11 Logging & Monitoring	Requires monitoring security logs to detect suspicious activities
12 IT Asset Control	Requires preventing unauthorized access of IT assets to AdZillah’s IT System and network not owned by AdZillah

Relevant controls according to risks have been analyzed in Table 11:

Table 11. Risks & Relevant Control Analysis

№	Risk Summary	Relevant Control Analysis
1	The server room is running hot and there is a lot of expensive devices in the company included server room devices that can catch on fire	Relevant control is 7. As a result, devices will be protected from damage and failure, probability of fire occurrence will be reduced.
2	Not having installed fire and anti-theft alarm can cause serious hazards to human life There is a risk of theft in company	Relevant controls are 7 & 9. Importance of having fire and theft alarm increases security. Participation in security trainings, increase knowledge on this kind of threats also will be beneficial.
3	Having unauthorized access to the central server and AdZillah IT System	Relevant control is 12. It contains physical security actions in addition to logical security in order to prevent both physical and logical unauthorized access.
4	Not using a secure remote access VPN increases confidentiality and unauthorized access risks	Relevant controls are 5 & 6. Control provides connection from a distance via remote access IPsec VPN, and security of the encryption algorithms being used is important.
5	Passwords the users use to access internal web-system can be weak and it increases risk of unauthorized access	Relevant controls are 4 & 6. Using a complex password and encryption service is another approach to strength passwords
6	Having access of partner to emails which can contain confidential data of company included customers' data	Relevant control is 10. NDA contract between parties must be signed to ensure keeping confidentiality.
7	NDA is not signed between parties in addition to general agreement to guarantee data confidentiality	Relevant control is 10. NDA contract between parties must be signed to ensure keeping confidentiality.
8	Not having a BYOD policy to add personally owned devices to BYOD program to monitor increases company security risks	Relevant controls are 8 & 12. It prevents access from devices which are removed from the policy such in case of employee termination.
9	Not having configured RAID technology in the server increases all data loss in case of hard drive failure Temperature in server room can reduce server running efficiency, or device failure	Relevant controls are 3 & 7. It provides RAID 5 level technology to back up data, and control 7 takes measure to protect devices
10	There are not procedures to provide non-stop working operation in case of disaster	Relevant controls are 1 & 2. They provide a regular risk assessment in every 3 years & preparation DRP

4.5 Determination of Risk Likelihood

In this step, a high, medium and low likelihood ratings are assigned to each identified risk in previous steps. The rating is assessed based on a subjective judgment.

Likelihood ratings are assigned as high, medium and low as shown table 12 below:

Table 12. Definitions of Risk Likelihood

Effectiveness of Controls	**Probability of Threat Occurrence**		
	High	**Medium**	**Low**
Low	High	High	Medium
Medium	High	Medium	Low
High	Medium	Low	Low

Risk likelihood ratings are described in Table 13 below:

Table 13. Ratings of Risk Likelihood

№	**Risk Summary**	**Risk Likelihood Evaluation**	**Risk Likelihood Rating**
1	The server room is running hot and there is a lot of expensive devices in the company included server room devices that can catch on fire	There are no procedures to control server room temperature, effectiveness of control is low, probability of fire is also low	Medium
2	Not having installed fire and anti-theft alarm can cause serious hazards to human life There is a risk of theft in company	There is not an installed fire and theft alarm in the company, it makes effectiveness of control low, likelihood of threat occurrence is also low due to physical security	Medium
3	Having unauthorized access to the central server and AdZillah IT System	Effectiveness of control to prevent unauthorized access to the server is medium, probability of unauthorized access is also medium	Medium

4	Not using a secure remote access VPN increases confidentiality and unauthorized access risks	Effectiveness of control not using a secure remote access VPN is low because employees use remote access VPN almost daily, likelihood of unauthorized remote access is also medium	High
5	Passwords the users use to access internal web-system can be weak and it increases risk of unauthorized access	Effectiveness of control in passwords the users use to access internal web-system is low as there are not password policy, and probability of threat occurrence is also low due to physical security protection in server room	Medium
6	Having access of partner to emails which can contain confidential data of company included customers' data	Effectiveness of control having access of partner to emails is low as there is not a special point in contract between them or not having an NDA contract, probability of occurrence is medium due to partnership since the company established	High
7	NDA is not signed between parties in addition to general agreement to guarantee data confidentiality	Effectiveness of control in outsourcing is low as they have not signed NDA, likelihood of occurrence is medium due to cooperation since the company established and not having trust issue between them	High
8	Not having a BYOD policy to add personally owned devices to BYOD program to monitor increases company security risks	There are not procedures to control personally owned devices in company and it make effectiveness of control low, probability of threat occurrence is also low due to having only 4 employees in the company	Medium
9	Not having configured RAID technology in the server increases all data loss in case of hard drive failure Temperature in server room can reduce server running efficiency, or device failure	Not having configured RAID technology in the server makes effectiveness of control low, and probability of occurrence is high due to temperature in the server room, and it increases device failure risk	High
10	There are not procedures to provide non-stop working operation in case of disaster	Not having procedures to provide business continuity non-stop makes effectiveness of control low, and probability of threat occurrence is medium due to location of the company	Low

4.6 Analysis of Risk Impact

In this step it will be assigned a high, medium and low impact ratings to each of risks identified in previous steps. Impact rating is determined according to analysis of likelihood occurrence and strictness of result.

Impact ratings are assigned as high, medium and low as shown table 14 below:

Table 14. Definitions of Risk Impact Rating

Magnitude of Impact	Definition of Impact
Low	May result in one or more of the following: 1) failure of some assets; 2) noticeably reputational damage to AdZillah.
Medium	May result in one or more of the following: 1) injury to human life; 2) interruptions in availability, integrity and confidentiality of assets; 3) reputational damage to AdZillah.
High	May result in one or more of the following: 1) death or severe injury to human life; 2) unrecoverable failure of assets, or loss of confidential data; 3) significantly reputational damage to AdZillah.

Risk impact ratings are shown in Table 15 below:

Table 15. Ratings of Risk Impact

№	Risk Summary	Risk Impact	Risk Impact Rating
1	The server room is running hot and there is a lot of expensive devices in the company included server room devices that can catch on fire	AdZillah IT System unavailable for use	High
2	Not having installed fire and anti-theft alarm can cause serious hazards to human life There is a risk of theft in company	Unauthorized disclosure or alteration of AdZillah IT System data	High

3	Having unauthorized access to the central server and AdZillah IT System	Unauthorized disclosure or alteration of AdZillah IT System data	High
4	Not using a secure remote access VPN increases confidentiality and unauthorized access risks	Unauthorized disclosure or alteration of AdZillah IT System data	High
5	Passwords the users use to access internal web-system can be weak and it increases risk of unauthorized access	Unauthorized disclosure or alteration of AdZillah IT System data	High
6	Having access of partner to emails which can contain confidential data of company included customers' data	Unauthorized disclosure or alteration of AdZillah IT System data	High
7	NDA is not signed between parties in addition to general agreement to guarantee data confidentiality	Unauthorized disclosure or alteration of AdZillah IT System data	High
8	Not having a BYOD policy to add personally owned devices to BYOD program to monitor increases company security risks	Unauthorized disclosure or alteration of AdZillah IT System data	High
9	Not having configured RAID technology in the server increases all data loss in case of hard drive failure Temperature in server room can reduce server running efficiency, or device failure	Unauthorized disclosure or alteration of AdZillah IT System data	High
10	There are not procedures to provide non-stop working operation in case of disaster	AdZillah IT System unavailable for use	High

4.7 Overall Determination of Risks

Overall risk determination will be conducted according to explanation in chapter 2.3.1. It is result of multiplication likelihood rating to impact rating. As a result, subjectively assigned numbers in scale of 1 – 100 will help to rank risks in order of severity and priority.

Table 16 indicates overall risk rating matrix:

Table 16. Overall Risk Rating Matrix

Risk Likelihood Rating	**Risk Impact Rating**		
	Low **10**	**Medium** **50**	**High** **100**
Low **0.1**	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10
Medium **0.5**	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
High **1**	Low 10 x 1 = 10	Medium 50 x 1 = 50	High 100 x 1 = 100
Risk Rating Range: Low (1 – 10), Medium (11 – 50), High (51 – 100)			

Overall risk ratings table is described in Table 17 below:

Table 17. Overall Table of Risk Ratings

№	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating
1	The server room is running hot and there is a lot of expensive devices in the company included server room devices that can catch fire	Medium	High	Medium
2	Not having installed fire and anti-theft alarm can cause serious hazards to human life There is a risk of theft in company	Medium	High	Medium
3	Having unauthorized access to the central server and AdZillah IT System	Medium	High	Medium
4	Not using a secure remote access VPN increases confidentiality and unauthorized access risks	High	High	High
5	Passwords the users use to access internal web-system can be weak and it increases risk of unauthorized access	Medium	High	Medium
6	Having access of partner to emails which can contain confidential data of company included customers' data	High	High	High
7	NDA is not signed between parties in addition to general agreement to guarantee data confidentiality	High	High	High
8	Not having a BYOD policy to add personally owned devices to BYOD program to monitor increases company security risks	Medium	High	Medium
9	Not having configured RAID technology in the server increases all data loss in case of hard drive failure Temperature in server room can reduce server running efficiency, or device failure	High	High	High
10	There are not procedures to provide non-stop working operation in case of disaster	Low	High	Low

4.8 Recommendations

The purpose of recommendations in risk assessment is to reduce identified risks in previous steps and minimize residual risks in an acceptable level.

Table 18 indicates recommendations:

Table 18. Table of Recommendations

№	Risk Summary	Risk Rating	Recommendations
1	The server room is running hot and there is a lot of expensive devices in the company included server room devices that can catch fire	Medium	Company needs to install a cooling system at server room to control the temperature
2	Not having installed fire and anti-theft alarm can cause serious hazards to human life There is a risk of theft in company	Medium	Need to install fire and anti-theft alarm, and requires secure card-key access system not to allow unauthorized person to get access private areas
3	Having unauthorized access to the central server and AdZillah IT System	Medium	Need to increase security measures on company firewall.
4	Not using a secure remote access VPN increases confidentiality and unauthorized access risks	High	Configuring remote access IPsec VPN
5	Passwords the users use to access internal web-system can be weak and it increases risk of unauthorized access	Medium	Using a complex password combination of letters, numbers and special characters, to add two factor authentications
6	Having access of partner to emails which can contain confidential data of company included customers' data	High	NDA must be signed between parties to keep confidential data a trade secret
7	NDA is not signed between parties in addition to general agreement to guarantee data confidentiality	High	NDA must be signed between parties to keep confidential data a trade secret
8	Not having a BYOD policy to add personally owned devices to BYOD program to monitor increases company security risks	Medium	Need to prepare BYOD policy to prevent access from devices which are removed from the policy such in case of employee termination.
9	Not having configured RAID technology in the server increases all data loss in case of hard drive failure Temperature in server room can reduce server running efficiency, or device failure	High	One recommendation is to use separate databases in case of attack not to lose all data. Other recommendation is to use RAID 5 level technology in server hard drives to back up data.
10	There are not procedures to provide non-stop working operation in case of disaster	Low	Need to prepare a disaster recovery plan

4.9 Documentation of Results

The final step is documentation of results gathered in previous steps in a risk assessment matrix and it is described in Table 19 below:

Table 19. Risk Assessment Matrix

№	Vulnerability	Threat	Risk	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating	Analysis of Relevant Controls	Recommendations
1	Temperature in the server room	Fire Hardware failure	Availability of AdZillah IT System and data	The server room is running hot and there is a lot of expensive devices in the company included server room devices that can catch on fire.	Medium	High	Medium	Relevant control is 7. As a result, devices will be protected from damage and failure, probability of fire occurrence will be reduced.	Company needs to install a cooling system at server room to control the temperature
2	Fire and anti-theft alarm	Fire Theft of equipment	Availability of AdZillah IT System and data	Can cause serious hazards to human life There is a risk of theft in company not having an installed anti-theft alarm	Medium	High	Medium	Relevant controls are 7 & 9. Importance of having fire and theft alarm increases security. Participation in security trainings, increase knowledge on this kind of threats also will be beneficial.	Need to install fire and anti-theft alarm, and requires secure card-key access system not to allow unauthorized person to get access private areas
3	Internal network security	Unauthorized access or use	Confidentiality and Integrity of AdZillah IT System data	Having unauthorized access to the central server and AdZillah IT System	Medium	High	Medium	Relevant control is 12. It contains physical security actions in addition to logical security in order to prevent physical and logical unauthorized access.	Need to increase security measures on company firewall.

Table 19. Risk Assessment Matrix (continued)

№	Vulnerability	Threat	Risk	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating	Analysis of Relevant Controls	Recommendations
4	VPN security	Unauthorized access or use	Confidentiality and Integrity of AdZillah IT System data	Not using a secure remote access VPN increases confidentiality and unauthorized access risks	High	High	High	Relevant controls are 5 & 6. Control provides connection from a distance via remote access IPsec VPN, and security of the encryption algorithms being used is important.	Configuring remote access IPsec VPN
5	Password strength	Unauthorized access or use	Confidentiality and Integrity of AdZillah IT System data	Passwords the users use to access internal web-system can be weak and it increases risk of unauthorized access	Medium	High	Medium	Relevant controls are 4 & 6. Using a complex password and encryption service is another approach to strength passwords	Using a complex password combination of letters, numbers and special characters, to add two factor authentications
6	Email server	Industrial espionage	Confidentiality and Integrity of AdZillah IT System data	Having access of partner to emails which can contain confidential data of company included customers' data	High	High	High	Relevant control is 10. NDA contract between parties must be signed to ensure keeping confidentiality.	NDA must be signed between parties to keep confidential data a trade secret
7	IT Outsourcing agreement	Industrial espionage	Confidentiality and Integrity of AdZillah IT System data	NDA is not signed between parties in addition to general agreement to guarantee data confidentiality	High	High	High	Relevant control is 10. NDA contract between parties must be signed to ensure keeping confidentiality.	NDA must be signed between parties to keep confidential data a trade secret

Table 19. Risk Assessment Matrix (continued)

№	Vulnerability	Threat	Risk	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating	Analysis of Relevant Controls	Recommendations
8	BYOD policy	Theft of equipment	Confidentiality and Integrity of AdZillah IT System data	Not having a BYOD policy to add personally owned devices to BYOD program to monitor increases company security risks	Medium	High	Medium	Relevant controls are 8 & 12. It prevents access from devices which are removed from the policy such in case of employee termination.	Need to prepare BYOD policy to prevent access from devices which are removed from the policy such in case of employee termination.
9	Data redundancy	Fire Unauthorized access or use	Confidentiality and Integrity of AdZillah IT System data	Not having configured RAID technology in the server increases all data loss in case of hard drive failure Temperature in server room can reduce server running efficiency, or device failure	High	High	High	Relevant controls are 3 & 7. It provides RAID 5 level technology to back up data, and control 7 takes measure to protect devices	One recommendation is to use separate databases in case of attack not to lose all data. Other recommendation is to use RAID 5 level technology in server hard drives to back up data.
10	Disaster recovery plan	Natural disaster	Availability of AdZillah IT System and data	There are not procedures to provide non-stop working operation in case of disaster	Low	High	Low	Relevant controls are 1 & 2. They provide a regular risk assessment in every 3 years & preparation DRP	Need to prepare a disaster recovery plan

4.10 Summary of Analysis and Result

As it clear from evaluations, risk assessment has been conducted through several steps. First and foremost, company IT assets have been identified and categorized as people, hardware and data after IT system of the company has been characterized. Identified assets also has been classified into sub-assets. The next step was to identify vulnerabilities and threats in order to find risks through pairing vulnerabilities and threats. Once risks have been identified, relevant control strategies have been listed and analyzed according to matched risks. Risk likelihood and impact ratings have been identified after control analyses has been completed. Risk ratings are found according to multiplication of likelihood and impact ratings. Relevant recommendations have been prepared in order to reduce identified risks and control residual risks. Finally, all collected data and results have been documented in a risk assessment matrix.

5 Conclusion

The research showed that AdZillah, as a fresh startup companies, has a number of threat risks on its IT System. Due to being a small-sized business, AdZillah's IT sytem has not invested enough on security solutions to protect its assets, operation and customers.

In order to identify the potential IT related risks, a risk identification and assessment activities were performed to identify the critical assets and vulnerabilities associated with each asset. It is deemed that this answers the first posed research question.

After the risk identification and assessment, appropriate controls were recommended in order to reduce the level of risks associated with each vulnerability. It is deemed that this answers the second posed research question.

Risk evaluation matrix is developed to define the level of risk by considering likelihood and impact analysis. This research work could be considered as a guidance for AdZillah IT System to strengthen its security in all levels.

Future work on this topic includes development of incident response and disaster recovery plans in consideration of cost and benefit analysis. In addition, choosing risk control strategy to control residual risks is also part of future work.

6 Future Work

Research of current work helped to gain necessary theoretical and practical skills to implement final step of risk management concept after completion the risk assessment. Choosing and implementation of a correct risk control strategy will help to minimize vulnerabilities and manage risks to an acceptable level.

Scope of the future planned work is described below:

6.1 Cost and Benefit Analysis

Cost-benefit analysis is often used by an organization to assess the appropriateness of a particular policy. Accurate profit-analysis identifies options that increase well-being in terms of benefits.

After IT risk assessment of AdZillah, each identified and accepted vulnerability will be analyzed not to experience company a huge amount of financial loss.

Planned task is to perform a cost benefit analysis (CBA) considering the information provided in risk assessment matrix and suggest the countermeasure that fits best based on conducted risk assessment results.

6.2 Incident Response Plan & Disaster Recovery Plan

Incident and disaster classification of the identified and described events in risk assessment matrix is the first step to decide on preparation of either incident response plan is required or a disaster recovery plan.

Importance of both plans aimed to ensure non-stop business continuity; however, the term business continuity is often associated with disaster recovery.

Overall, future planned work scope is to conduct CBA and preparation of IR or DR Plans.

Bibliography

[1] Lemos, R., 2002. Security guru: Let's secure the Net | ZDNet. [online] ZDNet. Available at: <https://www.zdnet.com/article/security-guru-lets-secure-the-net/> [Accessed 9 May 2021].

[2] Smart Eye Technology. 2021. Confidentiality, Integrity, & Availability: Basics of Information Security | Smart Eye Technology. [online] Available at: <https://smarteyetechnology.com/confidentiality-integrity-availability-basics-of-information- security/> [Accessed 10 May 2021].

[3] 2012. Principles of Information Security. 4th ed. Boston: Michael E. Whitman, Herbert J. Mattord.

[4] Vacca, J., 2017. Computer and Information Security Handbook. 3rd ed. Cambridge.

[5] Mineur, J., 2017. Why the risk matrix must die. [online] Medium. Available at: <https://medium.com/@JornMineur/why-the-risk-matrix-must-die-620a7287e7c> [Accessed 29 April 2021].

[6] Rowley, J., 2013. 5th Edition PMBOK® Guide—Chapter 11: Risk Strategies. [online] 4squareviews. Available at: <https://4squareviews.com/2013/08/09/5th-edition-pmbok-guide-chapter-11-risk-strategies/> [Accessed 29 April 2021].

[7] UCF Online. 2020. Business Continuity vs. Disaster Recovery: 5 Key Differences. [online] Available at: <https://www.ucf.edu/online/leadership-management/news/business-continuity-vs-disaster-recovery/> [Accessed 13 May 2021].

[8] Streefkerk, R., 2019. Qualitative vs. Quantitative Research | Differences & Methods. [online] Scribbr. Available at: <https://www.scribbr.com/methodology/qualitative-quantitative-research/> [Accessed 10 May 2021].

[9] 2006. Information Technology Risk Management Guideline. Virginia: Virginia Information Technologies Agency.

[10] Stoneburner, G., Goguen, A. and Feringa, A., 2002. Risk Management Guide for Information Technology Systems. Virginia: National Institute of Standards and Technology.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis

I Fuad Budagov

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Information Technology Risk Assessment of the Indoor Advertising Platform AdZillah”, supervised by Mohammad Tariq Meeran

   1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

   1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

17.05.2021