MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ZAPORIZHZHIA NATIONAL UNIVERSITY

FACULTY OF MATHEMATICS

Department of Computer Science

MASTER'S QUALIFICATION THESIS

on the topic: **«CYBER SECURITY THREATS ANALYSIS AND ESTABLISHMENT OF THE SECURITY RECOMMENDATIONS FOR THE INFORMATION SYSTEM ASSETS»**

Presented by student 2nd year, group 8.1223-z
speciality 122 Computer Science
(code and speciality name)
educational program Computer Science
(name of educational program)
A. Vasylchenko
(initials and surname)

Supervised by Associate Professor at the Department of Computer Science, Docent, Candidate of Technical Sciences (Ph.D) K. Reshevska
(position, academic title, last name, initials)

Reviewed by Associate Professor at the Department of Software Engineering, Docent, Candidate of Physico-Mathematical Sciences (Ph.D) V. Horbenko
(position, academic title, last name, initials)

Zaporizhzhya – 2024

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ZAPORIZHZHIA NATIONAL UNIVERSITY

Faculty of Mathematics

Department Computer Science

Educational Degree Master's Degree

Speciality Computer Science
(code and name)

Educational Program Computer Science

APPROVED
Deputy of the Head of the Department of Computer Sciences, Doctor of Technical Sciences, Professor
_____ G. Shylo
(signature)

" 12 " 03 2024

A S S I G N M E N T

FOR STUDENT'S QUALIFICATION

Vasylchenko Antonina
(name, surname)

1. Topic of the work Cybersecurity Threats Analysis and Establishment of the Security Recommendations for the Information System Assets

supervisor of the work K. Reshevska, Associate Professor at the Department of Computer Sciences, Docent, Candidate of Technical Sciences (Ph.D)
(surname, first name, academic title)

approved by ZNU order of « 01 » March 2024 № 384-c

2. Date of submission of the student's work 02.12.2024

3. Initial data for work 1. Problem statement.
2. Reference.

4. Contents of the settlement and explanatory note
1. Problem statement.
2. Analysis of the components of information security.
3. Development and establishment of the recommendations to remediate unacceptable risks.

5. List of graphic material (with precise indication of mandatory drawings)
presentation

6. Work sections consultants

Chapter	Consultant's last name, initials and position	Signature, date	
		the task was given	the task was accepted

7. Issue date of the task 11.03.2024

C A L E N D A R P L A N

№	Names of the stages Master's Qualification Work	Terms of the execution of the work	Note
1.	Plan development.	20.08.2024	
2.	Collection of raw data.	01.09.2024	
3.	Proccessing of methodological and	14.09.2024	
	teoretical sources.		
4.	Development of the first and second	01.10.2024	
	chapters.		
5.	Development of the third chapter.	09.11.2024	
6.	Forming and standard control of	28.11.2024	
	Master's Qualification work		
7.	Defence of Master's Qualification work.	14.12.2024	

Student _____ A. Vasylchenko
(signature) (initials and surname)

Supervisor _____ K. Reshevska
(signature) (initials and surname)

Passed standard control

Standard controller _____ O. Spitsa
(signature) (initials and surname)

РЕФЕРАТ

Кваліфікаційна робота магістра «Аналіз кіберзагроз та формування рекомендацій безпеки для активів інформаційної системи»: 52 с., 1 рис., 6 табл., 16 джерел, 1 додаток.

АКТИВ, АУДИТ, ВРАЗЛИВІСТЬ, ЗАГРОЗА, КОНТРОЛЬ, ОЦІНКА РИЗИКУ, РИЗИК, УСУНЕННЯ РИЗИКУ.

Об'єкт дослідження – кіберзагрози інформаційної системи.

Мета роботи: провести аудит з кібербезпеки невеликої компанії з метою виявлення та аналізу загроз в її інформаційній системі та заходів щодо їх запобігання.

Предмет дослідження – засоби контролю кібербезпеки для впровадження в інформаційну систему невеликої компанії.

Методи дослідження – порівняння, аудит, аналіз.

Проведений аудит та оцінка ризиків невеликої компанії виявили, що організації з обмеженим бюджетом стикаються з труднощами під час проведення оцінки ризиків і визначення надійних заходів безпеки для попередження загроз інформаційної системи компанії.

Виклики, з якими стикаються невеликі компанії, були підтверджені під час проведення внутрішнього аудиту та процедури оцінки ризиками.

Рекомендації, розроблені в проекті, а також виконана процедура оцінки ризиків підтвердили гіпотезу про те, що невелика компанія зазвичай має обмежений бюджет і не в змозі проаналізувати потенційні ризики та визначити відповідні засоби контролю безпеки, які рекомендовані міжнародними стандартами кібербезпеки.

Конкретні рекомендації щодо кібербезпеки пропонуються як частина майбутнього плану усунення ризиків з метою покращення стану кібербезпеки в організації.

SUMMARY

Master's Qualification Thesis "Cyber Security Threats Analysis and Establishment of the Security Recommendations for the Information Security Assets": 52 pages, 1 figure, 6 tables, 16 references, 1 supplement.

ASSET, AUDIT, CONTROL, RISK, RISK ASSESSMENT, RISK SCORE, RISK TREATMENT, THREAT, THREAT ACTOR, VULNERABILITY.

The object of the study – cybersecurity threats of the information system.

Aim of the study: to conduct a cybersecurity audit of a small-sized company in order to identify its information system's threats and measures of their prevention.

The subject of the study – cybersecurity controls for implementing it into the information system.

Methods of research: comparison, audit, analysis.

The conducted cybersecurity audit and risk assessment of the small size company revealed that the organizations with a tight budget face difficulties while conducting risk assessment and defining robust security measures for threats prevention of the information system of the company.

The challenges that small-size companies meet were confirmed while conducting internal audit, assessment procedure, and risk treatment planning.

The recommendations developed in the project as well as performed risk assessment procedure confirmed the hypothesis that small size company usually with a tight budget and which does not have proper cybersecurity department is not able to analyze potential risks and define appropriate security controls that are recommended by the international cybersecurity standards to eliminate weaknesses in the company's IT infrastructure and avoid the most widespread attacks on its information system.

Specific cybersecurity recommendations are proposed as a part of the future risk treatment plan in order to improve the cybersecurity posture of the organization.

TABLE OF CONTENTS

Assignment For Student's Qualification 2
Реферат 4
Summary 5
Introduction 8
1 Analysis Of The Components Of Information Security 11
1.1 Theoretical Aspects Of Cybersecurity Field 11
1.2 Main Principles Of It Auditing 13
1.3 Comparison Of The International Cybersecurity Standard And Framework 16
1.4 Conclusions To Chapter 1 18
2 Risk Assessment Procedure 19
2.1 Preparation 19
2.2 Risk Identification 21
2.3 Risk Analysis 25
2.4 Risk Evaluation 31
2.5 Conclusion To Chapter 2 32
3 Development And Establishment Of The Recommendations To Remediate Unacceptable Risks 33
3.1 Risk Treatment Planning 33
3.2 Risk Treatment Implementation 36
3.3 Established Cybersecurity Recommendations 37
3.3.1 Authentication Information 37
3.3.2 Remote Working 37
3.3.3 Security Of Assets Off-Premises 38
3.3.4 Secure Authentication 39
3.3.5 Protection Against Malware 39
3.3.6 Management Of Technical Vulnerabilities 40

3.3.7 Information Backup 40
3.3.8 Redundancy Of Information Processing Facilities 41
3.3.9 Networks Security 41
3.3.10 Segregation Of Networks 42
3.4 Assessing Residual Risks 42
3.5 Conclusion To Chapter 3 45
Conclusion 46
Reference 47
Supplement A List Of Information Security Controls 49

INTRODUCTION

Drastic development of technologies has led the world to facing a new era of challenges. The revolutionized inventions have not only increased the efficiency and accuracy of the work operations, but resulted in the rise of a new type of war – cyber war and a new type of crimes – cybercrimes.

All types of businesses and organizations which provide services and products via the Internet have automatically become the targets to the threat actors, who utilize various technologies in order to disrupt business operations, steal confidential data and/or corporate assets and destroy a company's reputation. So there is a growing demand for information security and proper protection of stored data against unauthorized access with a criminal intent. The World Economic Forum highlighted the issues of cybersecurity as companies, organizations have faced IT outage, and a great number of passwords leaked in data breaches [1].

So in the days of immutable technological progress, the actuality of cyber defense stands as a priority for any size of companies – from the organization with 2-3 employees to large worldwide corporations. But the issue of information system security for small and medium-sized companies is extremely important because of their tight budgets, lack of specially trained staff.

According to Dr. Jane LeClair who is the Chief Operating Officer at National Cybersecurity Institute, “Fifty percent of small to medium-sized businesses (SMB) have been the victims of cyber attack and over 60% of those attacked go out of business” [2, 10]. The NSBA research showed that a high number of attacks is possible due to the inability of the small to medium-sized businesses to defend their company’s assets from the adversaries. It is pointed out that the main reason is the lack of resources to implement security measures and absence of the cybersecurity awareness among organization’s employees [2].

The issues of cyber security and the system of its formation are highlighted in the works of Ukrainian researchers: S.Lehominova [3], H.Haidur [3], O. Kryvoruchka, D. Hnatchenko [4]. The issue of regular and systematic audit of the

security system of the organization is pointed out in the work by O.Ulichev and V.Petrashko [5]. The methodology of cybersecurity policy is pointed out by I.Diorditsa [6].

The problems of cyber threats and risk assessments are analyzed in the works of foreign scientists: A.Banerjee [7], J. LeClair [2], O. Matthew [8] and others.

The purpose of the research is to conduct a cybersecurity audit of a small-sized company in order to identify its information system's threats and measures of their prevention. In the context of the work it is important to determine whether the small-sized company with limited resources can implement the robust security measures. As a result of the analysis, it will be possible to define controls that are needed to be implemented to eliminate weaknesses in the company's IT infrastructure.

The object of the research is cybersecurity threats of the information system.

The subject of the research is cybersecurity controls for implementing into the information system of the small-sized company.

In order to reach the aim of the research the following tasks were established:

- to define the main components of the information system in the security area;
- to compare the world-known cybersecurity standards;
- to select the most appropriate standard for the organization with the limited resources;
- to perform an IT audit to identify critical assets and vulnerabilities;
- to conduct a cybersecurity risk assessment procedure which includes risk identification, analysis and evaluation;
- to select appropriate controls to reduce unacceptable risk score from the proposed cybersecurity controls;
- to develop recommendations for a risk treatment plan.

The structure of the project. Master's Qualification Thesis consists of introduction, three chapters, conclusion and a reference. The first chapter compares the international cybersecurity standards. The second chapter outlines the risk

assessment procedure. The third chapter specifies the developed recommendations to remediate unacceptable risks. The conclusion outlines the result of the research.

1 ANALYSIS OF THE COMPONENTS OF INFORMATION SECURITY

1.1 Theoretical aspects of cybersecurity field

For successful development and establishment of the recommendations for any size organization, but in our study particularly for the small-sized company, it is important to understand the crucial aspects of the information security area. In our research we take definitions of the glossary proposed by the Computer Security Resource Center of the National Institute of Standard and Technology in the USA [9] as it is one of the most influential institutions in the field of security. These definitions are the main components that are used during the whole cycle of the cybersecurity assessment and we are sure it is important to highlight them for our research.

So, the main concept under consideration is cybersecurity. According to the mentioned above glossary, *cybersecurity* represents the process of protecting and restoring information system components as well as preventing any hazards that could affect them [9]. In this frame, experts of cybersecurity use the term compliance to say that companies' infrastructure meets the legal and regulatory requirements [10].

Thus cybersecurity is a domain in computer science that plays a crucial role in the development of any kind of organization. This domain includes various techniques and methods that are used to protect a company's corporate data and valuable resources.

The next component that is crucial to understand from the point of view of a cybersecurity approach is asset. *Asset* is determined as an any resource that belongs to the organization and is used to support businesses [9] That is, an asset is any physical (e.g. network equipment, laptops, office buildings) or logical (e.g. virtual machine, software, data) component that belongs to the company, holds value, and is used to support business processes.

Among the next elements we would like to pay attention to the interpretation of such components as a threat, risk.

So, *threat* can be characterized as any event that can have a harmful impact on the business operations of the company and any corporate assets through adversarial actions of an attacker [9]. In other words, any action that has malicious intent and harmful impact on the company's assets. The threat could be intentional (such as hacker's attack), or unintentional (e.g. earthquakes or other natural disaster). In order for the threat to be executed successfully, there must be vulnerabilities within the organization's assets. In this frame the experts often use the idea of a threat landscape [11].

Another important definition in developing cybersecurity recommendations accurately is risk. *Risk* is defined as a score that represents the potential impact and probability of the occurrence of the potential threat [9].

Thus, risk gives organization an opportunity to understand the extent to which organization is subjected to the potential threats and it is calculated by the evaluation of the probability and impact of the potential threat on the corporate assets.

According to the Computer Security Resources Center *vulnerability* is a weak spot in the information system components that can be used by an adversary to execute an attack [9]. The wide range of vulnerabilities are given by the National Vulnerability Database [12].

It is necessary to point out that the successful development of recommendations for protection of the company's assets requires the proper identification of the vulnerabilities that are possible for an attacker to exploit.

We are sure that knowing the vulnerabilities that are present in the information system of the organization makes it possible to apply correct security controls. So, control as one of the important features of security procedures is defined as the measures that can reduce risk score [9].

In other words, controls are the measures that are used to eliminate identified vulnerabilities. It is possible to outline preventive measures (such as blocking incoming traffic from unknown source), detective (such as utilizing Security

Information and Event Management System (SIEM) to monitor suspicious activity), and corrective (such as restoring backup copies of the data that was affected by a malware).

1.2 Main principles of IT auditing

According to the NIST glossary, an audit is a review and examination of the organization's information system in order to asset the accuracy of the implemented security controls in order to verify the compliance with existing policies and procedures [9]. This technique is the primary method that is used for assessing the maturity level of the security of any-size organization as well as in helping to define accurate and effective security measures. In order to understand the workflow of the research it is important to understand the way the security audit is performed.

The main resource that we would like to utilise in our study, provides explicit guidelines for IT audit is an International Organisation for Standardisation (ISO) 19001. This documentation outlines the requirements for the auditors who perform audits of the information system.

According to the instructions of ISO 19011 auditor is required to collect evidence that would be used to determine whether an organization has any non-conformities that can specify the weaknesses in the information system assets.

It is also important to note, that according to the international standard all the collected data and evidence that were used to produce audit findings should remain confidential between an auditor and organization. "Auditors should exercise discretion in the use and protection of information acquired in the course of their duties. Audit information should not be used inappropriately for personal gain by the auditor or the audit client, or in a manner detrimental to the legitimate interests of the auditee. This concept includes the proper handling of sensitive or confidential information." [13, 6] All information that was gathered during an audit should be protected at all times by the persons who performed the audit [13]. So there are several ways of performing an audit such as on-site and/or remote activity. While

conducting an audit an auditor should gather as much information as possible to identify the level of conformity.

According to the rules of auditing process there are different types of methods to gather information but we would like to consider the following ones as the most effective for this case:

- interviewing employees. This is one of the most popular ways to conduct an audit. It includes gathering information through communication with organization's representatives. By utilizing this method employees can describe the specific processes within organizations, which help to understand the business operations;
- observation of the activity. This method includes observation of the daily tasks that are performed by the employees. For example, observing how HR representatives perform onboarding procedures, or how the information security team handles an incident;
- documentation. Reviewing documentation can give valuable information to an auditor. He or she can understand whether an organization has established policies and procedures that help to maintain information security within an organization [13].

But at the same time we think we should add the necessity to review the present technological configurations for the small-sized company. For example, by observing firewall rules it is possible to make a conclusion whether an organization implemented preventive controls such as blocking incoming traffic from unknown sources.

It is necessary to emphasize that taking into account specifics of each organization it is possible to determine appropriate methods by which audit findings can be produced.

So once the means of the audit have been determined, it would be possible to select an appropriate cybersecurity tool that provides robust, world-known cybersecurity measures (controls) to eliminate the probability of potential incidents.

The next stage is scope identification. The company called ***Brustver*** has been selected as a target for our investigation as it suits our criteria (small-sized company, tight budget, and absent compliance department). The staff of the company includes 5 employees with the office in Prague, Czech Republic. ***Brustver*** is a rapidly growing start-up that provides consulting services in the cybersecurity domain. That is to say, the privacy of the corporate and customers' data is a key element for the organization. Additionally, its employees don't have experience in the compliance domain which makes it a perfect fit for identifying whether the small size organizations are able to assert their cybersecurity posture and establish appropriate measures to eliminate potential risks. Knowing the scope of the research, it is possible to determine that the audit is the main method for the security assessment of the *Brustver* company.

Since the company is actively seeking partnerships with international organizations, the world's most known cybersecurity standards and frameworks should be considered as they will help to reach the desired goal such as developing recommendations for the information system assets of *Brustver*.

Since Brustver is an organization that operates fully remotely, the interview and technical methods were selected to assess the security of the organization's assets.

One of the main advantages of using already produced cybersecurity tools is its defined solid requirements that organizations of any size can follow in order to implement cybersecurity measures within their company. It also provides security measures that businesses can select based on the context of their organization to reduce existing risks. Some of the standards provide additional guidance for implementation of cybersecurity controls.

Thus there are two options under consideration to perform future procedures:

- cybersecurity framework from the National Institute of Standard and Technologies – NIST CSF 2.0.;
- cybersecurity standard established by International Organization for Standardization – ISO 27001.

1.3 Comparison of the international cybersecurity standard and framework

In order to compare two tools that provide robust security measures, we have to analyse their features.

The first is the National Institute of Standard and Technologies Cybersecurity Framework. The National Institute of Standard and Technology (NIST) has developed the cybersecurity framework (SF). “The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts.” [14, i] The framework provides detailed guidelines on risk assessment and recommends specific controls that can be implemented to reduce identified risks. Although NIST CSF is widely used by organizations of all sizes, it is designed to give guidance on cybersecurity implementation rather than certify companies with a compliance standard.

The second tool is the International Information Security Standard 27001 issued by International Organisation for Standardization 27001 (ISO). ISO 27001 is “prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system.” [15, v] The following standard not only specifies the requirements the organization should fulfill, but also outlines 93 controls that any company has to walk through in order to select those that would reduce existing risks. This standard gives organizations of any size an opportunity to expand their scope, to strengthen brand reputation and trust of the customers and partners.

The detailed comparative analysis of the tools are presented in table 1.1 The table outlines the main features of the two instruments that are considered to be the most popular in the cybersecurity industry.

Table 1.1 –- Comparison of world known cybersecurity standard and framework

Feature	ISO 27001	NIST Cybersecurity Framework (CSF)
Issuing Organization	International Organization for Standardization (ISO)	National Institute of Standards and Technology (NIST)
Format	Designed as a compliance standard	Designed as a guide

Continuation of table 2.2

Feature	ISO 27001	NIST Cybersecurity Framework (CSF)
Purpose	Establishes an ISMS to protect information assets	Helps to reduce cybersecurity risk
Approach	Risk-based management of information security	Framework for improving cybersecurity resilience
Structure	Defined set of controls and processes	Voluntary, flexible framework with five key functions
Scope	Focuses specifically on information security and confidentiality, integrity, and availability (CIA) of information	Covers broader cybersecurity concerns, including IT, people, and processes
Adoption	Widely adopted globally, especially in Europe and Asia	Widely adopted in the U.S.
Sector focus	Broad focus, suitable for all industries and sectors	Primarily used in critical infrastructure sectors, but adaptable to any sector
Customer trust	Helps establish trust with customers, partners, and clients by demonstrating a commitment to safeguarding sensitive data	Enhances consumer trust
Competitive advantage	Direct differentiator in different sectors where data security is a key selling point	Doesn’t directly offer a competitive advantage
Marketing and Public Relations	Tangible asset that can be used in marketing materials	Since NIST CSF is not certifiable, there’s limited opportunity to use it as a marketing tool

After comparing the features it is possible to outline the following key points:

– ISO 27001 has a clearer, more direct impact on brand recognition due to its certification process and global visibility, making it a strong asset for companies seeking to demonstrate their commitment to information security;
– NIST CSF, while not certifiable, can still enhance a company's cybersecurity posture and help build trust, especially among technically-minded stakeholders or within specific industries, but it doesn't offer the same formal branding advantage as ISO 27001.

So, it is possible to identify the main criteria for choosing an appropriate cybersecurity instrument for ***Bruster*** company.

They are*:*

– a trustworthy relationship with clients and partners;
– potential cooperation with leading companies;
– safety of corporate and clients' data;
– continuous improvement of the information system.
– so after each cybersecurity tool was analyzed, it is possible to say that ISO 27001 would satisfy all the expectations of the Brustver company.

1.4 Conclusions to chapter 1

The main components of information security were analysed.

Adit methods were explored in order to identify suitable for conducting audits of the company.

The scope of the research was identified.

Due to the comparison of the two tools (NIST CSF framework and ISO 27001 standard) the applicable instrument that will be used for the further steps of our research were selected.

2 RISK ASSESSMENT PROCEDURE

2.1 Preparation

The preparation stage of the cybersecurity assessment includes familiarization with the context of the organization, its business purpose and operations in order to correctly identify all the assets that are used within the organization. After the company has successfully defined its purpose, business operations and assets it is possible to identify potential threats that could affect the functionality and existence of the company. In the final stage, the organization should perform vulnerability discovery – the phase that allows it to identify all the weaknesses within the information system. As a result of identification of these components as well as performing a risk assessment procedure, the company will be able to define the controls that are needed to be implemented to eliminate vulnerabilities. Successful identification of the cybersecurity controls as well as their implementation allow to reduce probability and impact of the potential threats.

There are many cybersecurity methods and techniques that allow businesses to reduce risks associated with potential threats. However, the most profound way is to utilize well-known practices that were developed by the international organizations such as International Organization for Standardization or National Institute of Standards and Technology. Since our research is based on the requirements of the ISO 27001 standard, we will use the ISO 27005 standard to guide through the risk management process.

In order to select the correct and effective security measures for an organization with a tight budget such as Brustver, it is necessary to conduct a risk assessment procedure. Risk assessment is a procedure that allows to assess the potential risks to which the organization might be exposed and, as a result, provide a list of recommendations to eliminate unacceptable risks. The risk assessment procedure can be based on any methodology that is appropriate for the context of the

organization, but regardless of the selected methodology there are 3 main stages that should be taken into account:

- risk identification;
- risk analysis;
- risk evaluation [16].

During the stage of risk identification it is expected to identify all the corporate assets that are used within an organization. The list of assets should be developed according to the sensitivity of data and criticality of an asset to maintain business-mission of an organization. While identifying assets it is important to mention that each asset should be considered separately because not every asset has the same level of impact. For example, workstations of employees who perform work tasks might not be as critical as workstations of the managers, who store all the confidential corporate data that is used to maintain the business operations. Another example is the sensitivity of the data. Type of data that is used by the marketing department is not as critical as data that represents confidential information of the employees, customers and/or partners. After defining a list of corporate assets, vulnerability identification follows. It is necessary to understand the degree to which a component of the information system is susceptible to the potential threat. Knowing the vulnerabilities will help to understand the potential threats that can produce future incidents. The list of threats can be specified by the company itself or by using any additional cybersecurity resources. It is important to note that each identified threat should relate to the type of an asset. For example, if the company works fully remote, physical threats that target office location are not applicable.

During the stage of analysis the company should calculate the probability and impact of the potential threat that was defined earlier. By multiplying two values it is possible to calculate risk score.

At the final stage an organization can determine risks that are unacceptable to the business. Unacceptable risks are identified by comparing risk score and the value that is outlined in the risk matrix. If the risk score is higher then the value of the acceptable risk it is possible to say that the risk must be urgently treated. Once an

organization knows the unacceptable risks, it can create a risk treatment plan which includes the selection of appropriate cybersecurity controls to reduce these risks.

2.2 Risk identification

During the risk identification phase, a risk assessment methodology was selected for conducting the risk assessment procedure. The standard ISO 27005 which outlines the specific steps an organization should perform to complete risk assessment procedure recommends two most common methodologies:

- asset-based approach;
- threat-based approach [16].

Asset-based approach is an approach for conducting a risk assessment procedure that is based on the assets that were identified. The main variables that should be considered for this method include asset name, identified vulnerability that is related to the specific asset, adversary action, probability of the adversary event can negatively affect an asset, and impact of the threat on the functionality of an asset. After knowing these main components it would be possible to calculate the level of the risks.

Threat-based approach is another approach for conducting a risk assessment procedure. Both approaches require the identification of corporate assets. However, the main difference between these two methods is that a threat based approach would be more suitable for the organizations who have a deeper understanding in the cybersecurity domain. It requires an organization to select the threats that are applicable to the components of the information system which is possible if an organization has sufficient knowledge of the cybersecurity threats and its connection to corporate assets.

Since the Bristver organization is a startup that does not have a large number of assets and doesn’t have specialists who are familiar with the ISO 27005 standard

procedure, it was chosen to conduct a risk assessment according to the asset-based approach. Thus, the following system components were identified:

- macOS workstation. It is an employee's laptop with macOS operating system that is used to perform work tasks;
- Windows 10 workstation. It is the laptop of the top management representative with Windows 10 operating system that is used for work tasks as well as performing critical tasks for business operations;
- hardware server. It is a distantly located server that has a deployed Proxmox hypervisor with two virtual machines;
- VM Ubuntu OS. It is a virtual machine with Ubuntu operating system that is used to maintain a corporate website;
- VM Debian OS. It is a virtual machine with Debian operating system that is primarily used for administrative tasks and maintaining SIEM Wazuh.

After identifying the assets comes the vulnerability discovery phase. Vulnerability identification can be carried out using a penetration testing technique (simulating attacker’s behavior in order to exploit the system or/and steal corporate data), or by checking the existing policies and configurations related to cybersecurity. Based on the Brustver organization context the vulnerability discovery phase was performed by communicating with representatives of the organization and obtaining the technical evidence by checking systems’ and software configurations.

As a result of the vulnerability identification it was possible to define the findings that are documented in table 2.1.

Table 2.1 – Audit findings

Findings	Asset
Outdated version of macOS	macOS workstation
Outdated version of Google Chrome	macOS workstation
OS auto updates are not configured. Outdated versions of Zoom and Adobe Acrobat Reader	macOS workstation

Spotify, GarageBand, SimCity 4 were found. They are not needed to perform work tasks	macOS workstation

Continuation of table 2.1

Findings	Asset
VPN is not configured. Workstation connects to the public networks regularly	macOS workstation
There are open ports that are not needed to perform work tasks (such as mySQL and Nessus)	macOS workstation
Passwords are not stored securely. Password policy and procedures are not established and not implemented	macOS workstation
There are no physical security measures to protect workstation while working remotely	macOS workstation
Counter-Strike, World of Tanks games were discovered	Windows 10 workstation
Mikrotik has outdated routerOS version	Windows 10 workstation
Password policy and procedures are not established and implemented	Windows 10 workstation
Anti-malware solution Microsoft Defender doesn’t have configured auto updates	Windows 10 workstation
It is possible to see that VMs on hardware server are not isolated according to their criticality	Hardware server
Incoming traffic from untrusted source is not restricted	Hardware server
There are no backups for website content	VM Ubuntu
Incoming traffic from untrusted sources is not restricted	VM Ubuntu
There are open ports that are not needed to perform work tasks	VM Ubuntu
Load balancing is not configured to provide data availability of the website content	VM Ubuntu
Incoming traffic from untrusted sources is not restricted	VM Debian
There are open ports that are not needed to perform work tasks	VM Debian

After all the audit findings were gathered, it is possible to identify potential threats that can affect the confidentiality, integrity and availability of the Brustver corporate assets. The list of assets as well as their vulnerabilities give enough context to specify the potential threats that might affect the functionality of the components. While identifying threats it is also important to note that each asset can be malleable to one or more potential threats. For example, an employee's laptop can be affected by physical threat such as equipment theft, technological threat such as data loss utilized by an attacker’s privilege escalation technique, operational threats such as absence of proper maintenance of the equipment due to lack of an employee’s professional qualification.

The result of the risk identification stage is the filled table 2.2 that consists of the identified assets, potential threats and their vulnerabilities. It will be used for the second stage of the risk assessment procedure such as risk analysis.

Table 2.2 – Identified assets, potential threats and vulnerabilities

Asset name	Threat	Vulnerability
macOS workstation	Unauthorized access	Presence of outdated software and operating system
macOS workstation	Unauthorized access	Patch installation is not performed regularly
macOS workstation	Unauthorized access	Presence of the software that is not needed for work operations and can be potentially harmful
macOS workstation	Unauthorized remote access	Connection to the public network Internet is not performed over secure channels
macOS workstation	Unauthorized remote access	Presence of insecure open ports and protocols
macOS workstation	Credential discovery	There is no password policy

macOS workstation	Credential discovery	Password rotation procedure is not implemented

Continuation of table 2.1

Asset name	Threat	Vulnerability
macOS workstation	Credential discovery	Authentication data is not stored securely
macOS workstation	Physical damage or theft	Physical security measures are not implemented
Windows 10 workstation	Unauthorized access	Presence of unwanted software
Windows 10 workstation	Unauthorized remote access	Outdated RouterOS
Windows 10 workstation	Credential discovery	Password rotation procedure is not implemented
Windows 10 workstation	Malware installation	Microsoft Defender antivirus auto updates are not configured
Hardware server	Malware installation	VMs are not isolated according to criticality
Hardware server	Unauthorized access	Incoming traffic is not restricted
VM Ubuntu	Ransomware	Backups are not performed
VM Ubuntu	Unauthorized remote access	Incoming traffic is not restricted
VM Ubuntu	Unauthorized remote access	Insecure open ports

2.3 Risk analysis

The next stage after risk identification is risk analysis. This stage consists of assessing the probability of an incident occurring and its level of impact on the asset. According to ISO 27005 standard, there are two common two approaches to perform risk assessment:

– quantitative;
– qualitative [16].

A quantitative approach is a process where the assessment of the probability of an incident occurring and the level of its impact is based on a mathematical approach.

A qualitative approach is an approach in which the assessment of the probability of an incident occurring and the impact is calculated using quality indicators.

For example, the probability of occurrence is “low”, “medium” or “high”, and the impact of the incident can be “low”, “medium” or “high”.

Using a qualitative approach simplifies the risk assessment procedure, which is relevant for organizations with limited time and a large number of assets. In turn, using a quantitative approach takes more time, but provides a more accurate risk assessment result.

Since the Brustver organization does not have a large number of assets and prioritizes the result with a detailed risk assessment, a quantitative approach to assess the likelihood and impact was chosen.

In order to calculate risk utilizing the quantitative approach, the following formula should be used:

$$Risk = Likelihood * Impact.$$

Likelihood refers to the probability of the event occurring and is rated on the scale from 1 to 5, where:

1 – very unlikely. The risk event may occur only in exceptional circumstances such as utilizing complex resources to execute an attack;

2 – rare. The risk event could occur at some time. For example, there are security measures implemented, so an attacker must wait for the certain conditions to happen in order to execute an attack;

3 – unlikely. The risk event might occur. There are certain cybersecurity measures implemented. However, the system has certain vulnerabilities that can be exploited by an attacker.

4 – likely. The risk event will probably occur in most circumstances. There are no cyber security measures implemented or their efficiency is not strong.

5 – very Likely. The risk event is expected to occur in most circumstances. The cybersecurity measures are not implemented; an attacker can easily gain access to the corporate data without utilizing advanced tools.

To determine the probability of risk, the following was taken into account:

- known vulnerabilities as a presence of vulnerabilities impacts the probability of the adversarial event. For example, it is likely that an attacker will target vulnerable assets since it is easier to gain access to the system by exploiting the known vulnerability. On the contrary, if an asset does not have any vulnerabilities, the probability of the hazard to occur is much lower;
- absence of security measures. Security measures hinder the penetration into the system as they serve as preventive control. In cases where an organization doesn't have implemented security measures the probability of the adverse event to happen is much higher;
- complexity of an attack. If an attack requires special techniques for an attacker to be used the probability of an attack is lower than the attack that can be exploited by the less-skillful threat actors;
- available resources. Probability of an attack that requires additional resources is much lower than the attack that can be performed by ordinary techniques that don’t require additional tools;

– history of incidents. If an attack happened earlier and there were no security measures implemented then the probability of an attack to happen again is high.

Impact refers to the severity of the hazard and consists of the potential consequences or damage that could occur because of an incident. The impact is rated from 1 to 5, where:

1 – very low. There is no significant impact on business processes; there is minimal damage to the finance and reputation of the organization;

2 – minor. There is limited disruption to the business functionality; the financial or reputational loss is minor;

3 – moderate. There is disruption to business functionality that can be recovered in the medium term; there is a significant financial loss and damage to the organization's reputation;

4 – significant. There is a long-term disruption to business operations; major financial loss and damage to the organization's reputation;

5 – extreme. The business operations are no longer running; the financial loss and reputation damage is massive.

To determine the impact of the hazard, the following should be taken into account:

– asset criticality. The impact of threat on business will be higher if an asset is more critical for the business operations;

– data criticality. Assets that store sensitive data will likely experience higher impact.

In other words, in order to identify the impact of the threat the following question should be asked: “What negative consequences will business operations experience if the selected asset will be damaged or destroyed?” It is possible to conclude that assets such as workstation with Windows 10 is more critical for business operations than workstation macOS since it is used by the top management to perform all critical business processes. On the other hand, damage to the macOS workstation will not stop business from operating. Additionally, a hardware server is

a critical component for Brustver as it contains virtual machines that are needed to conduct all the necessary business processes. Knowing assets' characteristics and taking into account specifics of calculating probability and impact it was possible to calculate the risk score for each identified asset. The result of the risk assessment can be found in the table 2.3.

Table 2.3 – Risk score

Asset name	Threat	Vulnerability	Likelihood	Impact	Risk score
macOS workstation	Unauthorized access	Presence of outdated software and operating system	4	3	12
macOS workstation	Unauthorized access	Patch installation is not performed regularly	4	3	12
macOS workstation	Unauthorized access	Presence of the software that is not needed for work operations and can be potentially harmful	4	3	12
macOS workstation	Unauthorized remote access	Connection to the public network Internet is not performed over secure channels	2	3	6
macOS workstation	Unauthorized remote access	Presence of insecure open ports and protocols	3	3	9
macOS	Credential	There is no	3	4	12

workstation	discovery	password policy			
macOS workstation	Credential discovery	Password rotation procedure is not implemented	3	4	12
macOS workstation	Credential discovery	Authentication data is not stored securely	3	4	12

Continuation of table 2.3

Asset name	**Threat**	**Vulnerability**	**Likelihood**	**Impact**	**Risk score**
macOS workstation	Physical damage or theft	Physical security measures are not implemented	4	3	12
Windows 10 workstation	Unauthorized access	Presence of unwanted software	2	4	8
Windows 10 workstation	Unauthorized remote access	Outdated RouterOS	3	5	15
Windows 10 workstation	Credential discovery	Password rotation procedure is not implemented	2	5	10
Windows 10 workstation	Malware installation	Microsoft Defender antivirus auto updates are not configured	2	5	10
Hardware server	Malware installatio	VMs are not isolated according to	3	5	15

	n	criticality			
Hardware server	Unauthorized access	Incoming traffic is not restricted	4	5	20
VM Ubuntu	Ransomware	Backups are not performed	4	5	20
VM Ubuntu	Unauthorized remote access	Incoming traffic is not restricted	4	5	20

End of table 2.3

Asset name	Threat	Vulnerability	Likelihood	Impact	Risk score
VM Ubuntu	Unauthorized remote access	Insecure open ports	4	5	20
VM Ubuntu	DoS and DDoS attacks	Load balancing is not utilized	4	3	12
VM Debian	Unauthorized remote access	Incoming traffic is not restricted	4	5	20
VM Debian	Unauthorized remote access	Insecure open ports	4	5	20

2.4 Risk evaluation

At the final stage of the risk assessment procedure the calculated risk score should be compared to the risk acceptance criteria. Risk acceptance criteria is a risk score that is accepted for the organization because it doesn't have damaging effect on the business. This risk score is defined by the risk matrix below (figure 2.4). As it is possible to see, all the risks that have a score 8 and higher are considered to be unacceptable to the organization and should be treated. Therefore, each risk score that was calculated during the previous step should be evaluated according to the risk matrix that is outlined below. As a result, Brustver organization faces 20 unacceptable risks that are ready to be treated in the following chapter.

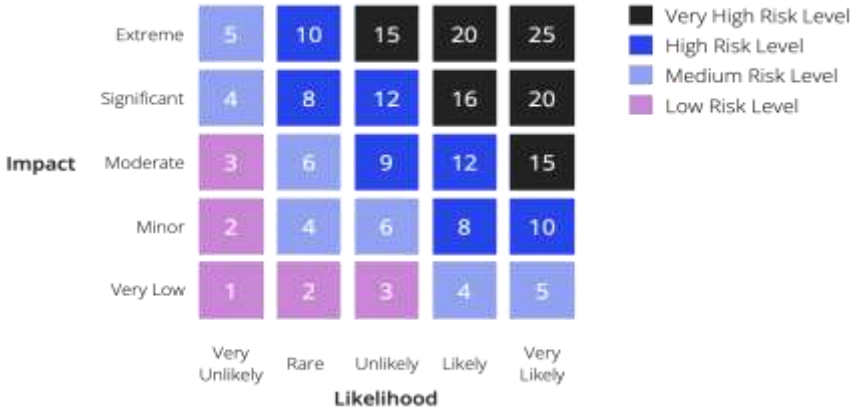


Figure 2.4 – Risk matrix

2.5 Conclusion to chapter 2

Risk identification was performed. It included identification of Brustver's assets, vulnerabilities, and potential threats.

Risk analysis was completed. It included the assessment of impact and likelihood of the potential threats and calculation of the risk score.

Risk evaluation was conducted. It included the comparison of the calculated risks with the established risk acceptance criteria. As a result unacceptable risks were identified for risk treatment procedures.

3 DEVELOPMENT AND ESTABLISHMENT OF THE RECOMMENDATIONS TO REMEDIATE UNACCEPTABLE RISKS

3.1 Risk treatment planning

After the risk assessment procedure was conducted and unacceptable risks were identified, it is possible to perform a risk treatment procedure. Risk treatment procedure is the process that allows organizations to select appropriate measurers for unacceptable risks. Since ISO 27001 was considered as a primary resource to conduct an audit and select appropriate security measures to eliminate critical risks, Annex A of the standard will be used.

Annex A of ISO 27001 consists of 93 controls that cover all types of threat including physical threats (such as theft of equipment) as well as technological (presence of insecure open ports, absence of antimalware solution or blacklisting for the corporate software to name a few).

To establish robust security measures all 93 controls were taken into account and selected those that were the most appropriate for the identified vulnerability. When selecting appropriate control to reduce risk level the following was considered:

- context of an organization. The selected control should match the context of organization such as a small size company that provides consulting services in the cybersecurity domain;
- cost-benefit aspect. The main goal of the risk management is not only to reduce risk level, but to perform it in a most cost-efficient way for organization;
- effectiveness of the control. Since the organization has a tigh-budget, all the selected controls should be effective, reducing the risk to acceptable level.

To sum up, it is possible to say that organization is primarily considers implementation of the most necessary solutions rather than implementing a wide

range of security measures. It is due to the fact that organization doesn't have a big number of employees to utilize security tools such as SIEM solutions and big budget to implement additional detective controls.

After taking into consideration the aspects above and considering all the controls that are documented in Annex A of ISO 27001 it is possible to develop a list of the critical risks that should be treated and the selected controls to reduce the level of risks. The result of the selected controls is displayed in table 3.1.

Table 3.1 – Selected controls to reduce risk level

Unacceptable risk	**Asset**	**ISO 27001 Annex A control**
Unauthorized remote access (incoming traffic is not restricted, presence of insecure open ports)	VM Debian	8.20 Networks security
Unauthorized remote access (incoming traffic is not restricted, presence of insecure open ports)	VM Ubuntu	8.20 Networks security
Ransomware (backups are not performed)	VM Ubuntu	8.13 Information backup
DoS and DDoS attack (load balancing is not utilized)	VM Ubuntu	8.14 Redundancy of information processing facilities
Unauthorized access (incoming traffic is not restricted)	Hardware server	8.20 Networks security
Malware installation (VMs are not isolated according to criticality)	Hardware server	8.20 Networks security 8.22 Segregation of

		networks

Continuation of table 3.1

Unacceptable risk	Asset	ISO 27001 Annex A control
Unauthorized remote access (outdated RouterOS)	Windows 10 workstation	8.20 Networks security
Credential discovery (password rotation procedure is not implemented)	Windows 10 workstation	5.17 Authentication information 8.5 Secure authentication
Malware installation (Microsoft Defender antivirus auto updates are not configured)	Windows 10 workstation	8.7 Protection against malware
Unauthorized access (presence of unwanted software)	Windows 10 workstation	8.7 Protection against malware
Physical damage or theft (physical security measures are not implemented)	macOS workstation	7.9 Security of assets off-premises
Credential discovery (there is no password policy, password rotation procedure is not implemented, authentication data is not stored securely)	macOS workstation	5.17 Authentication information 8.5 Secure authentication
Unauthorized remote access (presence of insecure open ports and protocols)	macOS workstation	6.7 Remote working 8.20 Networks security

End of table 3.1

Unacceptable risk	Asset	ISO 27001 Annex A control
Unauthorized access (presence of the software that is not needed for work operations and can be potentially harmful, presence of outdated software and operating system, patch installation is not performed regularly)	macOS workstation	8.7 Protection against malware 8.8 Management of technical vulnerabilities

3.2 Risk treatment implementation

The next step after selecting appropriate controls that are recommended by the International Organization for Standardization is to create a risk treatment plan.

Risk treatment plan specifies a concrete list of actions that should be performed by the employees of the organization to reduce the unacceptable level of risks. In our research, the result of the risk treatment plan will provide the cybersecurity recommendations for the organization that will help to understand whether the organizations with a tight budget are able to select appropriate cybersecurity measures without a proper cybersecurity department.

The recommendations are developed for 5 different assets taking into account identified vulnerabilities as well as a guide to the implementation of the selected control that is documented in the standard ISO 27002.

3.3 Established cybersecurity recommendations

3.3.1 Authentication information

Authentication information considers any information that is used for the purpose of authentication. This data is critical as its compromise can lead to the credential discovery and unauthorized access of an attacker to the corporate systems and network. According to ISO 27002 control 5.17 one way of mitigating the critical risks that is related to the insecure storage of authentication information is to incorporate usage of password managers among company's employees. Organization should define responsible individuals who should have access to the password managers for their work tasks. After defining such an individual it is necessary to verify that the master password is disclosed only to the authorized employees. It is also important to underline the establishment of the password policies and procedures. Such policy should cover:

- enforcing employees to use strong passwords. The password is considered strong when it consists of at least 16 symbols, capital letters, small letters, numbers and special symbols. In order to avoid brute force attacks, passwords should not include any words from a dictionary;
- implementing password rotation policy. To avoid credential compromise organization should enforce password rotation regularly;
- preventing usage of commonly used passwords or passwords that were used in the past;
- enforcing to change default passwords. All passwords that were proposed by the manufacturer of the equipment should be changed immediately.

3.3.2 Remote working

Even though remote working is a wide spread way of business operations it can potentially cause a lot of harm to the corporate assets: man-in-the middle attacks, data

leakage, APT to name a few. Since all of the Brustver employees work remotely it is important to establish policies and procedures to secure working while connecting to public networks. To reduce risks related to remote working according to the ISO 27002 control 6.7 the following should be implemented:

- implementing physical security measures for a corporate devices (such as kensington table lock);
- defining responsible personnel who can have an access to connect to the corporate devices remotely (e.g. using virtual desktop access);
- enforcing encryption of the assets that store corporate data;
- enforcing usage of secure data transferring protocols to avoid man-in-the-middle attacks (e.g. usage of corporate VPN to connect to the publicly available WiFi points);
- creating backups of the corporate data that is stored on the off-premises assets regularly to avoid data loss during an incident.

3.3.3 Security of assets off-premises

Another control that specifies guidance of the remote working is control 7.9. According to this control, organizations should protect assets that are located outside of the office facility. This will help to prevent equipment theft, data loss, and device compromise. The recommended actions to protect off-premises assets are:

- communicating with employees about the importance of not leaving corporate devices unattended;
- ensuring that third party is not able to view corporate information on the screen to avoid shoulder surfing attacks;
- implementing remote wiping of the corporate devices.

3.3.4 Secure authentication

In order to avoid unauthorized access and to make sure that authentication mechanism are secure it is important to implement additional level of security. Control 8.5 of ISO 27002 specifies that confidential data such as authentication information should be protected by additional measures. Such measures can include (but not limited to) multi factor authentication (MFA). Multifactor authentication allows organization to add additional level of security over their corporate assets. In case authentication information is compromised and an attacker gains access to the corporate account, multifactor authentication would ask an attacker to provide one more factor of authentication. Since this factor is considered to be a personal fact of an employee, an attacker is no longer able to gain an access to the system, even if he/she knows the corporate account credentials.

3.3.5 Protection against malware

Malware installation is a widely spread type of attack that can affect not only one component but to infect the whole corporate network that has all the corporate devices connected. In order to protect corporate data from malware organization should consider implementing ISO 27002 control 8.7 which specifies the actions an organization should take in order to protect their corporate assets from malware. Such actions include:

- deleting unnecessary software. Software that is installed on the corporated devices and is not used for performing work tasks can be potentially harmful as it can include trojan horse virus. Trojan horse virus is a malicious software that is installed into the legitimate software tricking users to think that software is actually benevolent;
- defining whitelisting. All the software that is needed for work tasks should be clearly defined by the top management representatives. All other

software that is to be installed should be reviewed by the responsible employee before installing it on the corporate device;

- updating anti malware solution regularly. All the updates that are proposed by the vendors should be automatically updated in order to eliminate the vulnerabilities that can be exploited by an attacker;
- Defining procedures for reacting to malware incidents. Organizations should make sure that employees are aware of their responsibilities and actions to be taken in case of malware infection. It will reduce the impact of malware on the corporate devices.

3.3.6 Management of technical vulnerabilities

Organization should ensure that there are procedures and polices implemented for managing vulnerabilities. According to ISO 27002 control 8.8 the employees of organization should gather information about new vulnerabilities and regularly conduct planned tests in order to identify vulnerabilities. Presence of outdated operating system as well as outdated software is potentially harmful as it includes known to an attacker vulnerabilities. Vulnerability management also includes:

- updating operation system to the latest version;
- configuring automatic updates from vendors;
- utilizing patch management solution to eliminate critical vulnerabilities in a timely manner;
- updating outdated software.

3.3.7 Information backup

To ensure that organization can continue operating during disaster it is important to implement backup policy. Control 8.13 of ISO 27002 specifies the guidelines on the backups of the corporate data. In order to implement data availability in case of ransomware attacks, all the data that includes websites content,

confidential information of employees, partners and clients should have backup copies to avoid losing critical data. Backup copies should also follow the following rules:

- being regularly created, tested and properly maintain to ensure that it can be restored in case of an incident;
- being stored at the facility that is geographically distant from the main site. For example, utilizing cloud technology or geographically distant data server;
- being protected by encryption. It is not enough to only create backups. It is also important to make sure that backup copies are protected by the means of encryption to ensure that data is kept confidential from unauthorized access.

3.3.8 Redundancy of information processing facilities

DoS and/or DDoS attacks are malevolent for the business operations since they threaten the availability of the data. When the critical data is no longer available an organization starts losing a lot of money since its business is no longer able to satisfy the needs of their customers. ISO 27002 control provides information regarding the redundancy of information facilities. According to this control, organization should implement redundant systems (e.g. redundant networks, duplicate components that are geographically separated, utilizing load balancing). After implementing load balancing for the corporate website organization will still have working website and more time to deal with malicious incoming traffic while being under attack.

3.3.9 Networks security

In order to avoid unauthorized access to the corporate assets it is extremely important to keep the network secure. Control 8.20 of ISO 27002 specifies the guidelines on the network security. Organization should make sure that all network

devices are properly maintained, only authorized personnel is able to access the corporate network, incoming and outgoing traffic is being monitored, traffic oncoming from the unknown sources is blocked, and vulnerable protocols and insecure ports (such as FTP, Telnet, HTTP, SNMP) are changed to secure alternative (e.g. SFTP, SSH, HTTPS, SNMPv3). Additionally, it is important to keep network services up to date. Therefore, routerOS that is used by mikrotik router should be updated to the latest version in order to eliminate the known to an attacker vulnerabilities associated with outdated version of routerOS.

3.3.10 Segregation of networks

One of the ways to protect critical components of the corporate infrastructure is to implement segregation of network. In case if the network is not segregated malware virus can not only infect one critical component, but to affect the whole network damaging all the corporate assets. Control 8.22 of ISO 27002 describes the best practices that are used in order to prevent the spread of malware. Organizations should implement network segregation in order to separate critical components (e.g. VM Ubuntu and VM Debian). Segregation can be performed according to the departments of the organization or criticality of the corporate asset. Responsible employees should also define rules for communication between components over the network. Where the component is not needed to communicate access to it as well as from it should be restricted.

3.4 Assessing residual risks

After establishing the security recommendations for the Brustver organization it is possible to asset residual risks. Residual risk is a risk that is left after implementing security controls. During the risk treatment procedure the final goal is to lower the unacceptable risk level to acceptable. Taking into consideration the

future implementation of the defined ISO 27002 controls during previous step residual risks are calculated by multiplying probability and impact of the threat. The values of residual risks can be found in the table 3.2.

Table 3.2 – Residual risk score

Asset name	Threat	Selected ISO 27002 control	Likelihood	Impact	Residual risk
VM Debian	Unauthorized remote access (incoming traffic is not restricted, presence of insecure open ports)	8.20 Networks security	1	5	5
VM Ubuntu	Unauthorized remote access (incoming traffic is not restricted, presence of insecure open ports)	8.20 Networks security	1	5	5
VM Ubuntu	Ransomware (backups are not performed)	8.13 Information backup	2	3	6
VM Ubuntu	DoS and DDoS attack (load balancing is not utilized)	8.14 Redundancy of information processing facilities	2	3	6
Hardware server	Unauthorized access (incoming traffic is not restricted)	8.20 Networks security	1	5	5
Hardware server	Malware installation (VMs are not isolated according to criticality)	8.20 Networks security 8.22 Segregation of	1	5	5

		networks			

Continuation of table 3.2

Asset name	Threat	Selected ISO 27002 control	Likelihood	Impact	Residual risk
Windows 10 workstation	Unauthorized remote access (outdated RouterOS)	8.20 Networks security	1	5	5
Windows 10 workstation	Credential discovery (password rotation procedure is not implemented)	5.17 Authentication information 8.5 Secure authentication	1	5	5
Windows 10 workstation	Malware installation (Microsoft Defender antivirus auto updates are not configured)	8.7 Protection against malware	1	5	5
Windows 10 workstation	Unauthorized access (presence of unwanted software)	8.7 Protection against malware	1	4	4
macOS workstation	Physical damage or theft (physical security measures are not implemented)	7.9 Security of assets off-premises	2	3	6
macOS workstation	Credential discovery (there is no password policy, password rotation procedure is not implemented, authentication data is not stored securely)	5.17 Authentication information 8.5 Secure authentication	1	4	4

End of table 3.2

Asset name	Threat	Selected ISO 27002 control	Likelihood	Impact	Residual risk
macOS workstation	Unauthorized remote access (presence of insecure open ports and protocols)	6.7 Remote working 8.20 Networks security	1	3	3
macOS workstation	Unauthorized access (presence of the software that is not needed for work operations and can be potentially harmful, presence of outdated software and operating system, patch installation is not performed regularly)	8.7 Protection against malware 8.8 Management of technical vulnerabilities	1	3	3

3.5 Conclusion to chapter 3

Risk treatment planning was performed.

Security controls were selected to eliminate unacceptable risks.

Recommendations to remediate threats that were analyzed previously were developed.

Residual risks were calculated taking into account future implementation of the security measures.

CONCLUSION

As a result of our study, the following was achieved:

- the main components of the information system in the field of security were identified (cybersecurity, compliance, asset, threats, risk, vulnerability);
- a comparative analysis of the well-known cybersecurity standards National Institute of Standards and Technologies Cybersecurity Framework and International Information Security Standard 27001 was conducted, which allowed us to determine the most effective methods of risk management;
- ISO 27001 was selected as the most acceptable standard for a small company with limited resources such as Brustver;
- an IT audit of the information system of a small organization Brustver was conducted. The audit allowed us to analyze threats and develop recommendations for preventing the occurrence of potential threats;
- a cybersecurity risk assessment procedure was conducted, which includes identification, analysis and assessment of risks;
- appropriate controls were selected, which are presented and characterized in the developed security recommendations for the information system assets of a small company. The established recommendations include 10 cybersecurity controls, which are developed for the further risk treatment plan of a small company.

The hypothesis was confirmed that an organization with a limited budget is not able to independently implement the requirements of the world-famous international standard ISO 27001, since the specified standard contains complex requirements that require a trained staff of employees who have sufficient knowledge and skills in the field of compliance, as well as a deep understanding of the standards ISO 27001, ISO 27002, ISO 27005. Since ISO 27001 is an approach based on risk assessment, it is difficult for companies that do not have compliance department and certified personnel to perform a risk assessment procedure and, as a result, determine the correct controls to eliminate these risks.

REFERENCE

1. World Economic Forum. (2024, July). Global IT outage : Top cybersecurity news this month. URL : https://www.weforum.org/agenda/2024/07/crowdstrike-global-it-outage-cybersecurity-news-july-2024/ (date of application : 31.08.2024).

2. The Impact of Cybersecurity on Small Business. (n.d.). URL : https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial1.pdf (date of application : 01.10.2024).

3. Lehominova, S., & Haidur, H. (2023). Analysis of Current Threats to the Information Security Organizations and the Formation of the Information Platform Against Them. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*. 2(22), 54–67. URL : https://doi.org/10.28925/2663-4023.2023.22.5467 (date of application : 03.10.2024).

4. Kryvoruchko, O., & Hnatchenko , D. (2024). Functional Features of an Intelligent Internal Audit Support System . *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*. 4(24), 40–49. URL : https://doi.org/10.28925/2663-4023.2024.24.4049 (date of application : 11.10.2024).

5. Петрашко, В., & Улічев, О. (2023). Дослідження існуючих підходів для створення безпечної мережі. *Молодий вчений*, 12 (124), 6-11. URL :https://doi.org/10.32839/2304-5809/2023-12-124-3 (date of application : 11.10.2024).

6. Діордіца І. Методологія дослідження кібербезпекової політики: кібернетичний, системний та матричний підходи. URL : http://yurvisnyk.in.ua/v4_2020/11.pdf (date of application : 11.10.2024).

7. Banerjee A., Malenfant J. (2024) Trelix Challenges the Status Quo with Responsible Security. URL : https://www.trellix.com/blogs/perspectives/secure-endpoints-with-industry-leading-platform/ (date of application : 22.10.2024).

8. Matthew Olney, The Top Four Challenges of Implementing Threat Detection and Responses: Why MDR Services Make a Difference.(2023). Open URL: https://insights.integrity360.com/the-top-4-challenges-of-implementing-threat-detection-and-response-why-mdr-services-make-a-difference (date of application : 23.10.2024).

9. National Institute of Standards and Technology. (n.d.). Computer Security Resource Center. National Institute of Standards and Technology. URL : https://csrc.nist.gov (date of application : 24.10.2024).

10. ISACA. (2020). ISACA glossary. ISACA. URL: https://www.isaca.org/ resources/glossary (date of application : 1.11.2024).

11. Rethinking Tactics 2022 Annual Cybersecurity Report. (2022). URL : https://documents.trendmicro.com/assets/rpt/rpt-rethinking-tactics-annual-cybersecurity-roundup-2022.pdf (date of application : 1.11.2024).

12. National Vulnerability Database. URL : https://nvd.nist.gov/vuln/categories (date of application : 2.11.2024).

13. Guidelines for auditing management systems (ISO 19011:2018). The British Standards Institution (2018). Published by BSI Standards Limited, P.48.

14. The NIST Cybersecurity Framework (CSF) 2.0. URL : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (date of application : 4.11.2024).

15. International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO.

16. International Organization for Standardization. (2022). ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks. ISO.

SUPPLEMENT A

List of information security controls

ISO/IEC 27002:2022 control identifier	Control name
5.1	Policies for information security
5.2	Information security roles and responsibilities
5.3	Segregation of duties
5.4	Management responsibilities
5.5	Contact with authorities
5.6	Contact with special interest groups
5.7	Threat intelligence
5.8	Information security in project management
5.9	Inventory of information and other associated
5.10	Acceptable use of information and other associated assets
5.11	Return of assets
5.12	Classification of information
5.13	Labelling of information
5.14	Information transfer
5.15	Access control
5.16	Identity management
5.17	Authentication information
5.18	Access rights

ISO/IEC 27002:2022 control identifier	Control name
5.19	Information security in supplier relationships
5.20	Addressing information security within supplier agreements

5.21	Managing information security in the ICT supply chain
5.22	Monitoring, review and change management of supplier services
5.23	Information security for use of cloud services
5.24	Information security incident management planning and preparation
5.25	Assessment and decision on information security events
5.26	Response to information security incidents
5.27	Learning from information security incidents
5.28	Collection of evidence
5.29	Information security during disruption
5.30	ICT readiness for business continuity
5.31	Legal, statutory, regulatory and contractual requirements
5.32	Intellectual property rights
5.33	Protection of records
5.34	Privacy and protection of PII
5.35	Independent review of information security

ISO/IEC 27002:2022 control identifier	Control name
5.36	Compliance with policies, rules and standards for information security
5.37	Documented operating procedures
6.1	Screening
6.2	Terms and conditions of employment
6.3	Information security awareness, education and training
6.4	Disciplinary process
6.5	Responsibilities after termination or change of employment
6.6	Confidentiality or non-disclosure agreements

6.7	Remote working
6.8	Information security event reporting
7.1	Physical security perimeters
7.2	Physical entry
7.3	Securing offices, rooms and facilities
7.4	Physical security monitoring
7.5	Protecting against physical and environmental threats
7.6	Working in secure areas
7.7	Clear desk and clear screen
7.8	Equipment siting and protection
7.9	Security of assets off-premises
7.10	Storage media
7.11	Supporting utilities
7.12	Cabling security

ISO/IEC 27002:2022 control identifier	Control name
7.13	Equipment maintenance
7.14	Secure disposal or re-use of equipment
8.1	User endpoint devices
8.2	Privileged access rights
8.3	Information access restriction
8.4	Access to source code
8.5	Secure authentication
8.6	Capacity management
8.7	Protection against malware
8.8	Management of technical vulnerabilities
8.9	Configuration management
8.10	Information deletion

8.11	Data masking
8.12	Data leakage prevention
8.13	Information backup
8.14	Redundancy of information processing facilities
8.15	Logging
8.16	Monitoring activities
8.17	Clock synchronization
8.18	Use of privileged utility programs
8.19	Installation of software on operational systems
8.20	Networks security
8.21	Security of network services
8.22	Segregation of networks

ISO/IEC 27002:2022 control identifier	Control name
8.23	Web filtering
8.24	Use of cryptography
8.25	Secure development life cycle
8.26	Application security requirements
8.27	Secure system architecture and engineering principles
8.28	Secure coding
8.29	Security testing in development and acceptance
8.30	Outsourced development
8.31	Separation of development, test and production environments
8.32	Change management
8.33	Test information
8.34	Protection of information systems during audit testing