Egyptian Informatics Journal 23 (2022) 383–404

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework

Khairur Razikin *, Benfano Soewito

Computer Science Department, BINUS Graduate Program, Master of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia

ARTICLE INFO

Article history:
Received 20 October 2021
Revised 16 February 2022
Accepted 7 March 2022
Available online 16 March 2022

Keywords:
Cybersecurity
Information technology
Security risk
Security hacking
ISO/IEC 27001

ABSTRACT

The proposed work was a recommendation model for designing cyber security decision support, in building an information technology security system based on risk analysis and the ISO/IEC 27001 cybersecurity framework. The proposed model aimed to obtain the best security system in mitigating security threats. This paper contributed to strategic policymakers in designing cyber security decision support recommendations to determine the best steps in designing information technology security systems. The model built can map the priority value of threat mitigation based on the relative threat score against the relative evaluation score of the implementation of ISO/IEC 27001 compliance. The mitigation priority value is the key in determining priority recommendations for building an information technology security system based on the ISO/IEC 27001 framework. Furthermore, the results implementation of information technology security system recommendations is tested by carrying out security attacks directly on the system being built. The work ends by conducting a statistical evaluation of the system built based on the recommendations of the information technology security system. The results achieved indicate an increase in the average value of the evaluation of ISO/IEC 27001 compliance from 36.27 to 82.37 with the p-value of Paired T-Test being 0.002138 < 0.05, meaning that there is a significant influence between threats to information technology security systems that implement and do not apply the recommendations of information technology security systems to the ISO/IEC 27001 compliance evaluation index value. Furthermore, based on 12 types of threat samples, it shows a decrease in the average threat criticality level from 8.75 to 4.00 with the p-value of the chi-square test being 0.0006605 < 0.05 and Fisher Test's p-value is 0.000008284 < 0.05, meaning that there is an association relationship between threats to information technology security systems that apply recommendations and do not apply recommendations to the criticality level of information technology security threats. While the results of the evaluation of the relationship between the implementation of security system recommendations on cybersecurity attack mitigation showed an increase in the effectiveness of cyber-attack mitigation from an average rating of 18.32 to 40.74 with the p-value of the chi-square test being 0.000005221 < 0.05 and the Fisher Test being 0.00000005658 < 0.05 means that there is an association relationship between systems that implement and do not implement recommendations based on ISO/IEC 27001 for cybersecurity attack mitigation.

* Corresponding author at: Bina Nusantara University, Kampus Anggrek, Jl. Raya Kb. Jeruk No. 27, RT.2/RW.9, Kb. Jeruk, Kec. Kb. Jeruk, Kota Jakarta Barat, Daerah Khusus Ibukota, Jakarta 11530, Indonesia.

E-mail addresses: khairur.razikin@binus.ac.id (K. Razikin), bsoewito@binus.edu (B. Soewito).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2022.03.001

1. Introduction

There had been a significant increase in security breaches and had to be wary of by the companies [1]. The record number of cybersecurity breaches exposed had risen by a staggering 36 billion in 2020. This was the worst year on record for information technology security [2]. Cybersecurity policymaking needed to be done properly so that security threats and attacks can be properly mitigated. From the perspective of technology and information security management, risk assessment and measurement of security readiness were an important part. Companies needed to implement risk management in information security to minimize the level of security risk and provide business continuity [3]. Every critical infrastructure had to implement an effective risk management process to protect stakeholders from financial, organizational, and reputational losses [4]. Cybersecurity framework had been proven to provide best practices in building security infrastructure and organizational systems [5].

We researched a public retail company with an on-premises and cloud-based information technology ecosystem that includes > 50 subsidiaries. The company had implemented a basic security system using a firewall and Antivirus. However, the security system that had been implemented had not been able to provide the best solution in detecting and preventing cyberattacks. Based on data in October 2020, the company received a security attack via email on one of the company's domains wherein 1 month there were 46,470 spam/phishing and 86 viruses/malware at inbound traffic. While the outbound traffic found 14,493 spams. Cybersecurity attacks also occurred in the form of brute force, which targeted 143,537 attacked on one of the company's servers. One of the causes of a cybersecurity breach was a security vulnerability in the system/application, of course, would be a way for attackers to perform cyberattacks. Security vulnerabilities could arise due to low compliance with the application of cybersecurity standards in system/application configurations that refer to the CIS benchmark, which is 46%. Several cybersecurity attacks had had an impact on the company's operational processes, such as disruption of the business communication system (email), cessation of transaction processing due to performance degradation, and information leakage. On the other hand, in one of its businesses the company was demanded by the regulator to be able to provide security guarantees for the platforms used in providing consumer services. So, it is very important to carry out risk analysis and build a security system with cybersecurity framework standards to get recommendations for the right security system as a mitigation measure against cybersecurity threats and attacks.

In previous research, the proposed risk analysis-based cybersecurity decision support model approach only involves financial factors and opportunities for threats without combining compliance with a cybersecurity framework that aims to reduce investment costs. Predictively this is effective in supporting cost-oriented decisions, but the decisions taken have not met the need for cybersecurity framework compliance [6–10]. In contrast, a decision support model approach based on a cybersecurity framework only focuses on implementing cybersecurity framework controls but does not involve the level of criticality of the existing threats. This makes it easier for policymakers to achieve compliance with the cybersecurity framework, but making decisions on security system development policies creates problems in the management of large investment costs [11–14]. The two approach models still create gaps for policymakers regarding the effectiveness of the recommendations from the previously proposed model. This occurs due to the unavailability of evidence on the effect of the previously proposed approach model on the system that adopts the model. In addition to the need from organizations for security system recommendations that can map priority levels based on threat criticality and following cybersecurity framework compliance, the limitations of the previous model are a motivation in building a cybersecurity decision support model that can present priority levels and provide convenience for policies stakeholders in determining mitigation measures according to the cybersecurity framework compliance roadmap.

This paper proposes a different approach from previous studies. The proposed approach is a combination of risk assessment and cybersecurity framework ISO/IEC 27001 to produce the best and most accurate recommendations for policymakers in making decisions on the development of information technology security systems. The model built can map the priority value of threat mitigation based on the relative threat score against the relative evaluation score of the implementation of ISO/IEC 27001 compliance. The mitigation priority value is the key in determining priority recommendations for building an information technology security system based on the ISO/IEC 27001 framework. The proposed model also provides a mapping of the ISO/IEC 27001 domain as well as threat mitigation priorities to make it easier for policymakers to make decisions. This approach is oriented to the extent to which a threat and the application of a cybersecurity framework can affect business continuity. This paper also provides a comprehensive analysis of the results of implementing recommendations for information technology security systems in the form of security testing on the system being built. The paper ends by conducting a statistical evaluation of the system built based on the recommendation of an information technology security system using the proposed model to obtain a significant level (p-value) between the system conditions before and after the implementation of information technology security system recommendations. The author raises 2 cases to find out the relationship between differences in system conditions before and after the implementation of security system recommendations where this case has never been presented in previous studies in the design of information technology security systems.

Case 1: Does the threat to the information technology security system affect the value of the risk level and the value of the security index?

Case 2: Does the information security system based on ISO/IEC 27001 have an effect in mitigating cybersecurity attacks?

The case is presented in the form of experiments and statistical analyses of companies operating in the retail industry. A research scheme with real steps in a company like this has never been done before. There are 3 contributions made in this research, namely:

1. Cyber security decision support model in the design of information technology security systems that produces security system recommendations with mitigation priority values based on the level of threat risk and evaluation of cybersecurity framework compliance.
2. The proposed model has flexibility in developing risk management methods and other cybersecurity frameworks according to business needs.
3. This research provides real evidence of a result of the analytical method used so that the effectiveness of the analytical method in real business operations can be measured.

Furthermore, this paper will discuss 1. Introduction; 2. Definition and related work; 3. Methodology; 4. Results and Discussion, 5. Conclusions and Further Work.

2. Definitions and related work

In previous studies, several risk assessment methods had been developed but three methods were often used, namely NIST-SP

800–30, OCTAVE, and ISO/IEC 27,005 [15–19]. Meanwhile, there were several types of international cybersecurity framework standards such as ISO 27001 [19,20], NIST [18], PCI-DSS [21,22].

2.1. Cybersecurity risk using OCTAVE Allegro

In general, the method chosen to be used must be following the needs of the company. Of these existing methods, the OCTAVE method, perhaps the most well-known of the risk frameworks, comes in three possible variants, namely OCTAVE, OCTAVE-S, and OCTAVE Allegro. The newest product in the OCTAVE series is the Allegro, which feels lighter and takes a more focused approach than its predecessor. Although OCTAVE Allegro is a relatively new process, it appears to have progressed very rapidly [15]. These three methods are not complementary or substitute for each other. The use of these three methods is intended to meet the specific needs of OCTAVE users who wish to conduct risk assessments. The goal to be achieved by OCTAVE Allegro is a comprehensive assessment of the operational risk environment of an organization to produce better results without requiring extensive knowledge in risk assessment. This approach differs from the OCTAVE approach, in that OCTAVE Allegro focuses on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are affected by threats, vulnerabilities, and disruptions as a result.

There are four stages in OCTAVE Allegro, namely (see Fig. 1) [15]:

1. Building drivers, where companies develop risk measurement criteria that are consistent with organizational drivers (things that move organizations).
2. Create an asset profile, where the assets that are the focus of the risk assessment are identified and described, and container assets are identified.
3. Identify threats, where threats to assets (within the scope of their containers) are identified and documented through a structured process.
4. Identify and mitigate risks, where risks are identified and analyzed based on threat information, and mitigation plans are developed in response to these risks.

2.2. Cybersecurity framework ISO/IEC 27001:2013

In general, the standard cybersecurity framework method used must be appropriate to the type of organization's business. ISO/IEC 27001 is an international standard that provides best practices in information system security management that can be used universally. This standard adopts a process approach for establishing, implementing, operating, monitoring, assessing, maintaining, and improving information security. ISO/IEC 27001 has 114 controls grouped into 14 domain groups starting in Annex 5 to Annex 18. While annex 1 to annex 4 is the introduction and definition (see Table 1) [23].

Table 1
Annex ISO/IEC 27001:2013.

Annex	Domain Control	Control
5	Information Security Policies	2
6	Organization of Information Security	7
7	Human Resource Security	6
8	Asset Management	10
9	Access Control	14
10	Cryptography	2
11	Physical and Environmental Security	15
12	Operations Security	14
13	Communications Security	7
14	System acquisition, Development, and Maintenance	13
15	Supplier Relationships	5
16	Information Security Incident Management	7
17	Business Continuity Management (BCM)	4
18	Compliance	8

In this paper, the writers were mapping the 14 domain groups of ISO/IEC 27001 into a 5-dimensional framework. This dimension mapping is carried out following the organizational structure, where each department has different responsibilities.

The Governance factor evaluates the readiness of the form of information security governance along with the agencies/companies/functions, duties, and responsibilities of information security managers. The risk management factor evaluates the readiness to implement information security risk management as the basis for implementing an information security strategy. Framework factor evaluates the completeness and readiness of the information security management framework (policies & procedures) and its implementation strategy. The Asset management factor evaluates the completeness of securing information assets, including the entire cycle of use of these assets. The Technology aspect factor evaluates the completeness, consistency, and effectiveness of the use of technology in securing information assets.

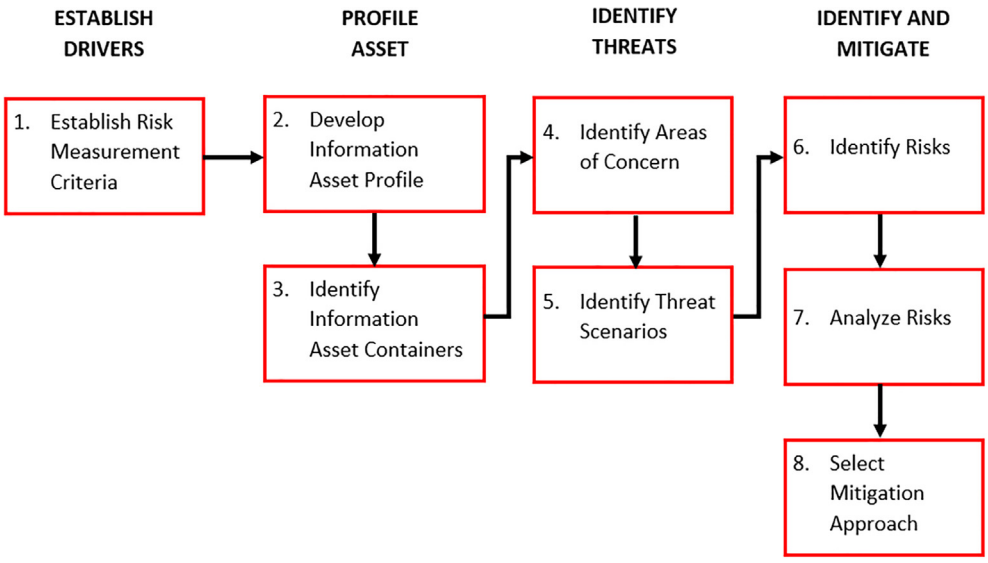

Fig. 1. Road Maps OCTAVE Allegro.

2.3. Cybersecurity attack

A cybersecurity attack is an attack carried out by virtual world criminals against one or several computers or networks. Maya attacks can be evil to deactivate computers, steal data, or use computers burglarized as launch points for other attacks. Virtual world criminals use various methods to launch a virtual world attack such as brute force, port scanning, malware, phishing, spam, ransomware, denial of service (dos), and other methods [24].

3. Research Methodology

In this study, we adopted the PDCA cycle (Plan do Check Action) for the stages of the problem-solving problem, where each cycle contains all activities in the study. The proposed method we place in the stage do, where the proposed method is a combination of risk analysis using the OCTAVE Allegro method and adherence evaluation of the cyber security framework ISO/IEC 27001. The combination of the two methods of analysis produces the priority value of mitigation for each security threat and mapping cybersecurity Framework ISO/IEC 27001.

3.1. Research stage

In building the recommendation of information technology security systems with best practices as supporters of the right and accurate cybersecurity decisions in mitigating cybersecurity threats, there are several stages we do, namely plan, do, check, act [25]

Plan stage, ideas, and formulations of research problems are discussed and developed, at this stage, we conducted literature studies on various related studies and models used in previous studies. Make the problem in the organization and determine the scope of research and mapping organizations. At this stage, we start planning models used in research and identifying organizational assets.

Do stage, is an analysis stage using the method proposed to produce cybersecurity recommendations as supporters of cybersecurity decisions by conducting Direct Observation and interviews with each Business Process Owner (BPO) asset technology. At this stage, Management also provides a decision on the list of recommendations that are implemented. This stage ends by implementing/developing safety recommendations that have been decided by the company's management.

The check stage is a testing stage on the results of the implementation and development that has been built. Tests are carried out directly against the system built on problems that exist in the organization.

Action Stage is an evaluation stage to find out the p-value between the system before and after the implementation of the recommendations is evaluated with the statistical analysis method by making hypotheses from research problems. Research ends by drawing conclusions hypotheses based on p-value in statistical tests.

3.2. Propose method

The proposed cybersecurity decision model is a model built by combining risk analysis and cybersecurity framework to produce security recommendations with the level of priority mitigation of security threats in every aspect of ISO/IEC 27001-based security. In this study, risk analysis was carried out using the OCTAVE Allegro method Because it is suitable for the scope of research, where research focuses on company information technology assets under the Management Department IT Infrastructure and does not require a broad contribution to all Department in the Experimental Company. So, Octave Allegro is very appropriate to find out how assets are stored, transported, and processed, and how they are influenced by threats, vulnerabilities, and interference as a result. While the cyber security framework ISO/IEC 27001 is used because ISO/IEC 27001 is the most appropriate type of information system security management certification for the company engaged in the Industrial Retail where the experimental company is done. In other cases, the proposed model can use other analysis method combinations according to the user's condition and business needs.

This model has 3 layers aimed at producing recommendations as supporters of cybersecurity decisions in designing a risk-based information technology security system and the cybersecurity framework. This recommendation has a mitigation priority value for each security threat and is mapped into the dimensions of the cybersecurity framework.

3.2.1. Requirement layer

This model requires 2 analytical methods, namely risk analysis and compliance analysis of Cybersecurity Framework. Risk analysis is needed to be able to find the existing security threat and map it into the level of criticality. While compliance analysis of the Cybersecurity Framework is needed to determine the extent of the organization to carry out governance with best practices based on the cybersecurity framework.

5. Risk analysis method. There are 8 steps in the OCTAVE Allegro method:

Step 1: Build Risk Measurement Criteria. Risk Measurement criteria need to be defined to obtain the impact of the area of a threat to information technology assets and map into the level of impact of threats. There are several parameters in building risk measurement criteria namely:

a. Impact of the area: As a result of a threat to the vision of the organization's mission and objectives that include reputation, financial, productivity, security, fines, and penalties.
b. Impact value: quantitative grade of the impact of specific risks of the organization in the Low, Medium, High, Very High category
c. Risk measurement criteria: a series of qualitative measures where the impact of each risk affects the vision of the mission and objectives of the organization that represents the value of the impact of a threat.

Each asset can have the same type of threat, but the level of criticality of these threats may be different for every asset.

Step 2: Develop asset profile information. Interviews with each party responsible directly for the use and managing of information technology assets need to be carried out to obtain information about the level of criticality of assets for organizational business operations, as well as factors for information technology assets.

Step 3: Identify asset container information. This step focuses on getting information about how these assets are stored, managed, or sent both Technical, Physical, and People factors.

Step 4: Identify the Area of Concern. In this step, the risk profile is developed by information technology assets by finding a component of threats from situations or conditions that might threaten the information technology assets owned. Development is made as detailed as possible and must still consider the specified security needs for information assets and how these assets can be affected by the threat when a real scenario is made. Area of Concern is made and used as the beginning of the development of risk profiles in the next step.

Step 5: Identify the risk of threats. In this step, start building a threat scenario which is a condition of information technology assets that can be threatened with danger to determine whether

a risk can affect information technology assets. Threat scenarios are compiled from unwanted actors, motives, tools, and results.

Step 6: Identify the risk. Conduct an assessment of risk impacts measured based on the Impact Measurement Criteria that has been made in step to 1. Any Area of Concern generates one or more consequences and will be assessed by the impact of the existing area.

Step 7: Analyze the risk. Perform the measurement of which parts of the organization are affected by the threat, by calculating the risk value for each risk to each information asset. This assessment is used to determine which risk requires mitigation steps as soon as possible and to prioritize mitigation actions. Risk value is a qualitative value given to describe the range of the impact that occurs against the organization when the threat scenario occurs.

Step 8: Choose a reduction approach. Determining which risk is mitigated and how to do it by giving a priority value to the risk and deciding on the approach in terms of risk mitigation based on the company's factors. The risk mitigation approach is divided into 3 choices [15], namely:

6. Accept, is a decision made at risk analysis not to act in risk handling and to accept the consequences caused. Received risks usually have a small impact on the company.

7. Mitigate, is a decision made at risk analysis to deal with risk by developing and implementing controls to oppose existing threats or to minimize the results of the impact caused. Mitigated risks are risks that have medium to high impacts on the organization.

8. Defer, is a situation where the risk is not accepted or mitigated based on the wishes of the organization to gather additional information and carry out additional analysis. The suspended risk is monitored and evaluated in the future. The suspended risk is usually a risk that has no significant impact on the organization.

9. ISO/IEC 27001 cybersecurity framework compliance evaluation

Evaluation is done by directly interviewing the person in charge of the information technology assets in the company. There are 5 sections of the interview (see Fig. 2), where each section has a different number of questions. Each interview question is given a choice of answers that have been given weights. The evaluation value of the section is the accumulated weighted value of all questions in that section, while the value of the compliance evaluation is the accumulated evaluation value of the entire interview section.

Section 1 is Governance. This section evaluates the readiness of the forms of information security governance within the organization, as well as the duties and responsibilities of information security management.

Section 2 is Risk management. This section evaluates the readiness to implement information security risk management as the basis for implementing an information security strategy.

Section 3 is the Framework. This section evaluates the completeness and readiness of the information security management framework (policies & procedures) and implementation strategies.

Section 4 is Information technology Asset Management. This section evaluates the completeness of safeguarding information assets, including the entire life cycle of those assets.

Section 5 is Aspects of technology and Information security. This section evaluates the completeness, consistency, and effectiveness of the use of technology in securing information assets (see Fig. 2).

Fig. 2. Evaluation Factor of ISO/IEC 27001:2013 Compliance.

3.2.1.1. Result mapping layer. In this layer, the results of the process in the requirements layer are displayed as a matrix. First, the risk matrix where every threat that exists in the asset has been mapped based on its criticality level and the mitigation approach. Second, the cybersecurity framework compliance evaluation matrix where each dimension has an achievement value that describes the implementation of the organization's compliance with the cybersecurity framework and the security gap for each dimension.

3.2.1.2. Correlation layer. This layer is the process of combining the results of the risk analysis and the compliance evaluation analysis of the cybersecurity framework. To get the mitigation priority value for a type of threat to the dimensions of the ISO/IEC 27001 framework, 2 variables are needed, namely the relative threat score and relative evaluation score.

10. The relative threat score is a value of the probability of occurrence that can be achieved by a threat to information technology assets. The greater the relative threat score of a threat, the higher the level of occurrence of threats to assets and the greater the impact received by the organization. The smaller the relative threat score, the smaller the level of occurrence of threats to assets and the smaller the impact received by the organization. The relative threat score is obtained from the weight value of a threat divided by the maximum value that each threat may have. The value of the weight of a threat is obtained by accumulating the number of assets affected by the threat to the level of threat criticality for the organization.

11. The relative evaluation score is the highest possible score for the implementation of cybersecurity framework compliance. The higher the relative evaluation score, the better the implementation of cybersecurity framework compliance in the organization. The lower the relative evaluation score, the worse the implementation of cybersecurity framework compliance in the organization is. The relative evaluation score is obtained from the results of the cybersecurity framework compliance evaluation in the previous layer.

To validate that the combination of the two analytical methods can work well, the results of the two analytical methods must have the same maturity level. The maturity level matrix consists of 4 levels, where level 1 is the lowest, namely "not feasible", level 2 is the "basic framework", level 3 is "good enough", and level 4 is "compliance". The higher the security evaluation value based on the cybersecurity framework compliance evaluation, the higher the maturity level value, the lower the threat risk level received by the organization. The lower the security evaluation value, the lower the maturity level, the higher the threat risk level received by the company. Each level of maturity level has an achievement contribution with a different percentage value for each type of threat and dimension of the cybersecurity framework.

4. Result and Discussion

In the Planning stage, responding to the increasing global security issues, we found that the increasing security threats also occurred in experimental companies. Then we started to map the problem and develop a strategy. At this stage, we also conducted a literature study of the solutions provided in previous studies. In addition, mapping of the organization is also carried out to obtain the right sources in carrying out the proposed solution (see Fig. 3).

4.1. Cybersecurity decision support model

There are 3 layers of processes that must be carried out in the proposed model (see Fig. 4), but first, it is necessary to identify all assets in the company. So, getting support from management is an important factor in achieving research success. We have identified assets obtained from interviews with related parties and are directly responsible for assets. The information technology assets under the management of the IT Infrastructure department in the on-premises datacenter consist of 11 hardware assets, 6 software assets, 4 system assets, and 5 information assets.

4.1.1. Requirement layer

The proposed model requires 2 types of analysis methods as the main requirement to be able to produce security system recommendations as a cybersecurity decision supporter. The method is a risk assessment method and evaluation of the implementation of cybersecurity framework compliance (see Fig. 4).

4.1.2. Risk analysis

Security threat risk assessment is carried out directly by meeting with several asset BPOs in the IT Infrastructure department and several related departments in the company. Detailed interviews were conducted to obtain information on important assets in operations. After the preparation is ready and the required data supports it, a risk assessment is carried out using the OCTAVE Allegro method which consists of eight steps.

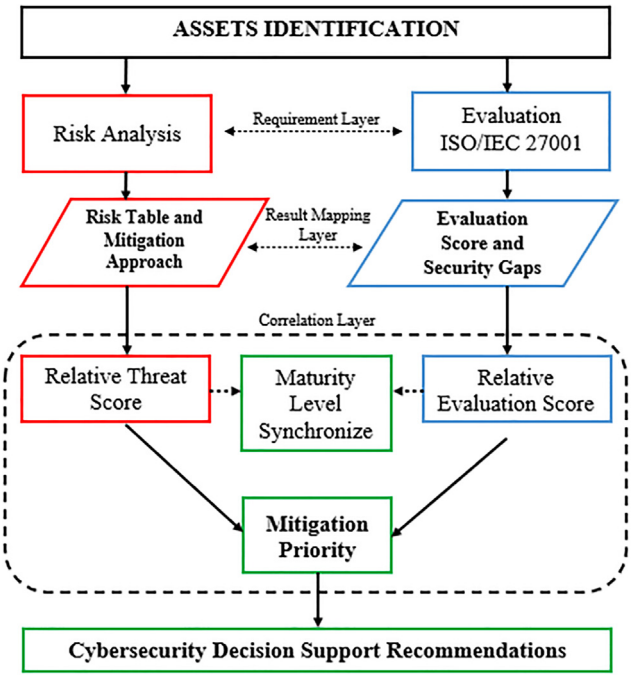

Fig. 4. Cybersecurity Decision Support Model.

Step 1 – Building Risk Measurement Criteria

Risk measurement criteria are parameters used to determine the level of impact in each threat area. In this study, we adopted

Table 2
Impact risk criteria.

Priority	Impact Area
5	Customer Reputation and Trust
4	Financial
3	Legal & Regulatory
2	Operational
1	Health and Safety

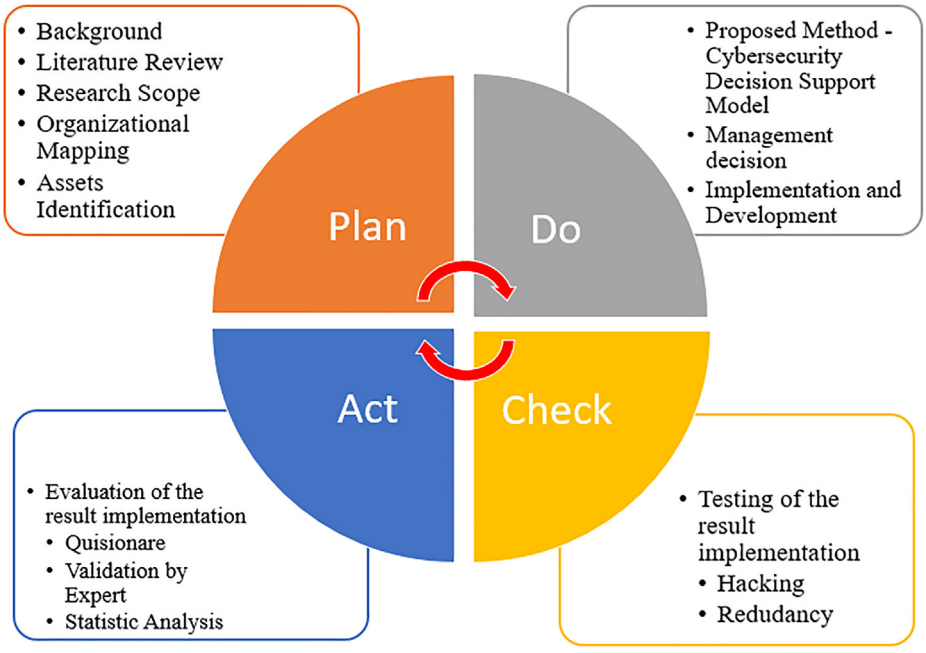

Fig. 3. Research Stage.

Table 3
Example risk impact criteria.

Priority	Impact Area	Low	Medium	High	Very High
5	Customer Reputation and Trust	Minor reputational sensitivity	Impact on company reputation but still manageable	Major reputational sensitivity	Significantly lost market share
		Service failure only to 1 customer.	Service failure to some customers.	Major service failure to one customer group	Major service failure to all customers in Holding Group

the risk measurement criteria from the Dept. Internal Audit and added the health and safety impact area (Table 2).

There are 5 Impact Areas, namely reputation and user trust, finance, fines and legal sanctions, productivity, and security and health. Each impact area has 4 levels of impact, namely Low, Medium, High, and Very High (see Table 3). Impact areas have different priority levels, where priority 1 is the lowest priority level and 5 is the highest priority level. The higher the priority level in the impact area, the more important the area factor is to the company .

Step 2 – Developing Asset Profile

Critical information technology assets are the most important technology and information assets for companies. The criteria used to determine whether an asset is a critical asset is if the company will be affected if (Table 4):

Furthermore, we collected data on critical information technology assets that exist in the company through interviews with the person in charge of these assets, we found 13 critical assets, namely (Table 5):

The further activity after determining the critical assets is to create an asset profile for each asset. The asset profile used is following the worksheet provided by OCTAVE Allegro. This worksheet is a detailed explanation of assets based on aspects of the rationale for selection, description, owner, security requirements, and most important security requirements (Table 6).

Table 4
Criteria of Threat.

No	Criteria of Threat
1	Leaked access to unauthorized individuals
2	Modified so that it can't be used
3	The problem caused by third parties
4	Natural disasters or human action (Flood, Fire, Explosion)
5	Permanently destroyed or temporarily lost

Table 5
Critical Asset.

Category	Asset ID	Asset
Hardware	HW1	Firewall Sophos SG330
	HW2	Firewall Sophos XG
	HW3	Firewall MIKROTIK
	HW4	Edge-Core Switch
	HW5	Router PBR SANGFOR
	HW6	Host Virtual Machine
	HW7	Storage
Software	SW1	Antivirus Sophos
System	S1	Email System
	S2	Database System
Information	I1	Information Access Server
	I2	Information Access Database
	I3	Information Access Email Account

Step 3 – Identifying Asset Container

The writers identify information asset containers which are places where assets are stored, moved, or processed. At this stage, we use the Worksheet information asset risk environment map where container assets are divided into 3 categories, namely:

Technical: Hardware, software, or systems that are under the company's control (internal), or outside the company's control (external).
Physical: A physical location or document that is under the company's control (internal), or outside the company's control (external).
People: Anyone who knows information that is under the company's control (internal), or outside the company's control (external) (Table 7).

Steep 4 - Identifying the Area of Concern

The writers started to document all possible conditions that could threaten the company's information technology assets. The following are the steps in defining areas of concern:

1. Conducting a review of each registered container to see potential areas of concern.
2. Document each area of concern defined in the Information asset risk worksheet.
3. Expanding the area of concern to generate threat scenarios.
4. Documenting how threats affect the security requirements for each information technology asset.
5. Continuing steps 1–4 for each container on the information asset risk environment maps and document as many areas of concern as possible.

In this step, we get 9 areas of concern for hardware assets, 6 areas of concern for software assets, 7 areas of concern for system assets, and 5 areas of concern for asset information (Table 8).

Step 5 - Identifying threat scenarios

At this stage, a threat scenario is created and more detailed about the property rather than the threat. The required activities are:

1. Completing the asset risk worksheet information for each identified threat scenario
2. Determining the probability into the description of the threat scenario created against the information asset risk worksheet.

Each area of concern is developed to obtain information that may have a relationship with the threat. An example of an area of concern in Table 9 is leaking access to unauthorized individuals,

Table 6
Example of asset profile.

Allegro Worksheet 8	***Critical Hardware Asset Profile***	
Critical Asset	***Rationale for Selection***	***Description***
Firewall Sophos SG	Possible access leaks, misconfiguration, and cyber-attacks can disrupt network performance and traffic.	Contains rules that allow or deny access in and out of the server network and the Internet, List of users/employees who can access VPN become the gateway for Private Tunnel VPN interconnection to the On Cloud Data Centre Network and Partners
Owner		
Holding Group		
Security Requirement		
Confidentiality	Only authorized officers can view asset information	
Integrity	Only authorized officers can modify asset information	
Availability	This asset must always be available for 24 h × 7 Days × 1 Month × 1 Year	
Most Important Security Requirement		
Confidentiality	*Integrity*	***Availability***

Table 7
Example of Container Assets Sophos SG.

Allegro Worksheet 9a	Information Asset Risk Environment Map (Technical)
Internal	
Container Description	Owner(s)
Applications: Web Access Management, Device management is managed and stored in the device access management web application. Web Access management hardcoded with physical assets.	Dept. IT Infrastructure
External	
Container Description	Owner(s)
Firmware: Operating System It is an operating system that functions as a security device powered by threat intelligence, AI, and machine learning from Sophos Labs and Sophos AI to secure users, networks, and endpoints from ransomware, malware, exploits, phishing, and various other cyberattacks.	Sophos Principle
Allegro Worksheet 9b	Information Asset Risk Environment Map (Physical)
Internal	
Container Description	Owner(s)
Physical Device Sophos SG: Data Center, to enter the Datacenter room, you must have the authority and be registered in the electronic key system	Dept. IT Infrastructure
VPN Tunnel Parameter Document, Interconnection between company or partner data centers via VPN Tunnel requires VPN Tunnel parameters. These parameters are stored in the VPN Tunnel Parameters document	Dept. IT Infrastructure
Backup Configuration File, the backup process is carried out and sent via email automatically within a daily timeframe. The email account of the recipient of the backup configuration document is registered on the asset device	Dept. IT Infrastructure
External	
Container Description	Owner(s)
–	–
Allegro Worksheet 9c	Information Asset Risk Environment Map (People)
Internal Personnel	
Container Description	Department or Unit
IT Network and Server	Dept. IT Infrastructure
IT Security and Compliance	Dept. IT Infrastructure
IT Infra Support	Dept. IT Infrastructure
External Personnel	
Container Description	Organization
IT support vendor is an officer appointed by management to provide support for device maintenance	PT. SHIFT

a threat can occur if IT employees as actors still use the default username and password in device management. This can happen because officers do not follow the hardware hardening security standards properly so that it can cause access leaks, the impact of access leaks can be disrupted, and even stop device functions due to configuration changes or modifications by unauthorized parties. To prevent this, change management procedures are needed to ensure that any changes that occur are carried out and prepared properly.

Step 6 - Identifying the risks

This stage is the credential that confirms or determines the threat the scenario impacts on the organization. The required activities are:

Table 8
Example Areas of Concern.

No	*Asset*	*Area of Concern*
1	Hardware	Loss of power supply due to temporary blackout or malfunction of power supply equipment
2		There is damage to the device components due to the period of use
3	Software	Application installation failure due to unsupported user device compatibility
4		Lack of control and supervision over the use of applications on work devices
5	System	System failure due to application/OS version update
6		Disruption of system performance due to abnormal activities using the system by the user
7	Information	User negligence due to writing username and password on physical/digital documents that are easily visible to the public
8		Using leaked passwords

Table 9
Example of the threat scenario.

Allegro Worksheet 11		Threat scenario – asset hardware – Sophos SG
1	*Information Asset*	Sophos SG
	Area of Concern	Access Leaked
	1. Actor	IT Staff
	2. Means	Using the default username dan password
	3. Motive	Does not comply with the hardware security standard
	4. Outcome	
	Disclosure	Yes
	Modification	Yes
	Destruction	No
	Interruption	Yes
	5. Security Requirement	Change Management and security configuration Assessment tools

1. Describe how the organization will be affected when a threat occurs.
2. Recording at least one potential consequence on the asset risk information worksheet. Others can be recorded if important. The recorded consequences must be very specific. The risk evaluation of the area impact criteria should be considered when examining the consequences (Table 10).

Step 7 - Analyzing the risks

This step focuses on how the level of risk is recognized. The activities required at this stage are:

1. Measuring the impact of risk and classifying it in severity (very high, high, moderate, or low) for each critical asset to the area of concern.
2. In this step, the relative risk score needs to be calculated and will be used for further analysis in helping the organization to decide on the best strategy in dealing with risk.

$$i = a.c \tag{1}$$

i	= Impact Score
a	= Impact Area Priority
c	= Impact Area Criticality

Table 11 is a relative risk score matrix that is used to calculate the overall value of the impacts that occur in all impact areas against

Table 10
Example of risk identification.

Allegro Worksheet 12		Risk Identification – Hardware Asset
Critical Asset		Sophos SG
Area of Concern		Access Leak
Risk	Consequence	• The decreased performance causes the device function as an Internet gateway to be disrupted • The device cannot be accessed or used • Production server network internet connection disconnection • Termination of business services • An internet access failure occurred on the production server • Abuse of internet access • Dependence on non-aggression support services on third parties causes the problem handling process to be hampered • Loss of Functionality of network security tools • Declining company revenue • Lowering customer trust
	Customer Reputation and Trust	Major service failure to one customer group
	Financial	25,000,001–50,000,000
	Legal & Regulatory	Complete information and documentation
	Operational	Operational activity shut down; the whole process is done manually for 12 h.
	Health and Safety	Employee health problems can be cured within 2 days because of increasing employee working hours

Table 11
Matrix relative risk score impact area.

Impact Priority	Impact Area	Low (1)	Medium (2)	High (3)	Very High (4)
5	Customer Reputation and Trust	5	10	15	20
4	Financial	4	8	12	16
3	Legal & Regulatory	3	6	9	12
2	Operational	2	4	6	8
1	Health and Safety	1	2	3	4

Table 12
Example of risk analysis.

	Critical Asset	*Area of Concern*	*Risk*			
1	Sophos SG	Access leak to an unauthorized individual	*Consequence severity*	Abuse of access rights that causes company data to leak		
				Impact Area	***Value***	***Score***
				Customer Reputation and Trust	High	15
				Financial	Medium	8
				Legal & Regulatory	Low	3
				Operational	High	6
				Health and Safety	low	1
				Relative Score		**33**

threat scenarios. The matrix value of an impact area is obtained from the multiplication of the priority value of the impact area to the weight value of the impact criticality value. For example, the impact area of reputation and customer trust has a priority value of 5, so if the impact of a threat has a Very High criticality value which has a weight value of 4, the score of a threat to an impact with a very high criticality is 5 × 4 = 20. The same method is carried out for each impact area on the criticality value of the impact on assets.

i = Impact Score
a = Impact Area Priority
c = Impact Area Criticality

Table 12 is an example that shows how the relative score is obtained. The relative score is obtained from the accumulation of the risk value of a threat scenario on assets against each impact area received by the company if the threat occurs. The risk value is obtained from the multiplication of the threat matrix of the area impact weight value to its criticality weight value as described in Table 11. In Table 12, there is a scenario of the threat of leakage of access to unauthorized individuals. This threat has a score on the impact of the reputation and customer trust area of 5 × 3 = 1 5, where 5 is the priority weight of the impact area and 3 is the high threat risk value with a weight of 3. While the impact on the financial area has a score of 4 × 2 = 8, in the impact on the area of fines and legal sanctions has a score of 3 × 1 = 3, the impact on the area of productivity has a score of 2 × 3 = 6, while the impact on the area of security and health has a score of 1 × 1 = 1, so the relative risk score of the leak threat scenario access for unauthorized individuals to critical assets of Sophos SG is 15 + 8 + 3 + 6 + 1 = 33.

Step 8 - Choosing a mitigation approach

In this step, the writers were sorting each discovered risk based on their risk rating. The identified risks are classified based on their relative risk scores:

Table 13 is a map of risk categories against the relative risk score obtained in step 7 along with the mitigation approach steps to threats. Threats to assets that have a relative risk score range of 46 to 60 are in risk pool 1 with an extreme risk category, and threats to assets that have a relative score range of 31 to 45 are in risk pool 2 with a major risk category, then the mitigation approach for both categories The risk for the threat is Mitigate, meaning that control will be carried out on the threat so that it can eliminate or reduce the possibility of consequences from the impact of the threat. Threats that have a relative score range of 16 to 30 are in risk pool 3 with a moderate risk category still being considered for mitigation or deferred, if mitigation is carried out, it will be carried out in the next IT project procurement program. Meanwhile, threats to assets with a relative risk score range of 0 to 15 are in risk pool 4 with the risk category in the Minor group being accepted, which means the company will not provide a budget for IT project procurement, as an alternative, the department can mitigate internal-based project procurement enhancements.

Table 13
Matrix risk core.

Risk Score	Risk Pool	Criticality Level	Mitigation approach
40–60	1	Extreme	Mitigate
30–45	2	Major	Mitigate
16–29	3	Moderate	Defer
0–15	4	Minor	Accept

4.1.3. Evaluation of the implementation ISO/IEC 27001:2013

Evaluation of the implementation of the ISO/IEC 27001:2013 cyber security standard is carried out directly by meeting the cross-departmental process business owner. The control domain of the ISO/IEC 27001 standard is classified into 5 factors, namely governance, risk management, framework, asset management, and technology aspect.

Furthermore, each factor has a different number of questions which are categorized into 3 parts. Each question has 4 answer choices where each answer in each section is given a different weight value (Table 14).

The mapping of the number of questions into 3 parts aims to determine the level of compliance with ISO 27001 in each dimension, where question part A is the minimum limit for the application of the security framework, part B is the middle limit for the application of the security framework, and part C is the maximum limit for the application of the security framework (Table 15).

Table 14
Answer choice weight score.

Respondent's Answer/Security Status	Weight of Section		
	A	B	C
are not done	0	0	0
In planning	1	2	3
In Application or Partially Applied	2	4	6
Full Applied	3	6	9

Evaluation Score (*es*) for each dimension is obtained by accumulating all the respondents' answer scores,

$$es = \sum des \tag{2}$$

des	$=(wa+wb+wc)+(xa+xb+xc)+(ya+yb+yc)+(za+zb+zc)$
des	= Dimensional evaluation score
w, x, y, z	= Total answer for each choice and section
a, b, c	= Weight for sections A, B, and C

Part C is available if the sum of the evaluation scores of part A and part B > of the threshold (t) the minimum score in part C, where

$$t = 2a + 4b \tag{3}$$

a	=	jumlah pertanyaan bagian A
b	=	jumlah pertanyaan bagian B

Table 16 shows the results of the number of respondents' answers for each answer choice on each dimension of ISO/IEC 27001.

4.1.4. Analysis result layer

In our proposed model, the analysis result layer is the second layer after the requirements layer (see Fig. 3). In this layer, the results of the analysis of the two requirements methods are presented in the form of a risk matrix and the value of the ISO/IEC 27001-dimension evaluation.

4.1.5. Result of risk analysis

In Table 17 we map the level of threat and risk for each asset based on the Asset ID (see Table 5), where each asset ID already has a threat type and risk level.

Visualization of the results of risk analysis can show the types of threats to assets based on the level of risk (see Fig. 5). Each Asset can have the same type of threat but with a different level of criticality. So, with the threat scenarios built, each critical asset will have 5 types of threat scenarios.

4.1.6. Result of evaluation ISO/IEC 27001 compliance

The results of the evaluation of compliance with ISO/IEC 27001 are an illustration of the extent to which information technology management controls based on ISO/IEC 27001 are implemented by the organization. ISO/IEC 27001 information technology management controls are mapped within the dimensions of the ISO/IEC 27001 framework (see Fig. 2) (Table 18).

Each dimension has a maximum score that can be achieved by the organization so that gaps can be mapped which can be described through cybersecurity gaps (see Fig. 6).

4.1.7. Correlation layer

Security recommendations based on mapping and threat mitigation priorities as support for cyber security decisions are a combination of the results of risk analysis and evaluation scores of the implementation of ISO/IEC 27001 Standards that have been carried out in the previous stage. The mitigation priority value of the com-

Table 15
Question matrix.

Dimension	Governance			Risk Management			Framework		
Section	A	B	C	A	B	C	A	B	C
Question	8	8	6	10	4	2	12	10	7
Total	22			16			29		
Dimension	**Asset Management**			**Technology Aspect**					
Section	**A**	**B**	**C**	**A**		**B**		**C**	
Question	24	10	4	14		10		2	
Total	38			26					

Table 16
Respondent's Answer Results.

Dimension	Governance			Risk Management			Framework			Asset Management			Technology Aspect		
Total Question	22			16			29			38			26		
Respondent's Answer	Section			Section			Section			Section			Section		
	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
are not done (w)	1	1	2	0	0	0	0	0	0	0	0	1	0	1	1
in planning (x)	3	4	4	8	1	2	10	8	4	14	5	3	7	2	1
in the application or partially applied (y)	3	3	0	1	1	0	0	0	3	5	2	0	6	7	0
full applied (z)	1	0	0	1	2	0	2	2	0	5	3	0	1	0	0
Evaluation Score	32			31			44			75			57		

Table 17
Mapping threat and risk level by asset.

Threat		Minor	Moderate	Major	Extreme
THREAT	Access Leak (AL)	SW1	HW2, HW6, HW7, S2, I1, I3	HW1, HW3, HW4, HW5, S1, I2	-
	Modification (M)	SW1	HW1, HW2, HW6, HW7, S2, I1, I3	HW4, S1	-
	Problem Cause by the Third party (PTP)	HW2, I1, I2	HW1, HW2, HW6, HW7, I3	S1, S2	-
	Disaster (D)	HW2	-	HW1, HW3, HW4, HW5, S1, S2	HW6, HW7
	Destroy or temporarily lost (D/L)	HW2, I1, I2	I3	HW1, HW3, HW4, HW5, S1, S2	HW6, HW7
Mitigation Approach		**Accepted**	**Defer**	**Mitigate**	**Mitigate**

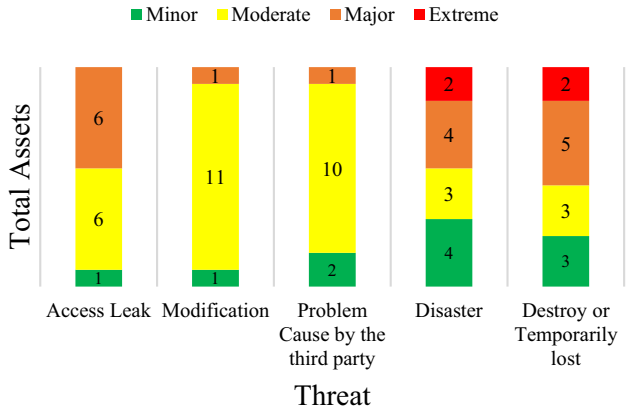

Fig. 5. Result of Risk Analysis.

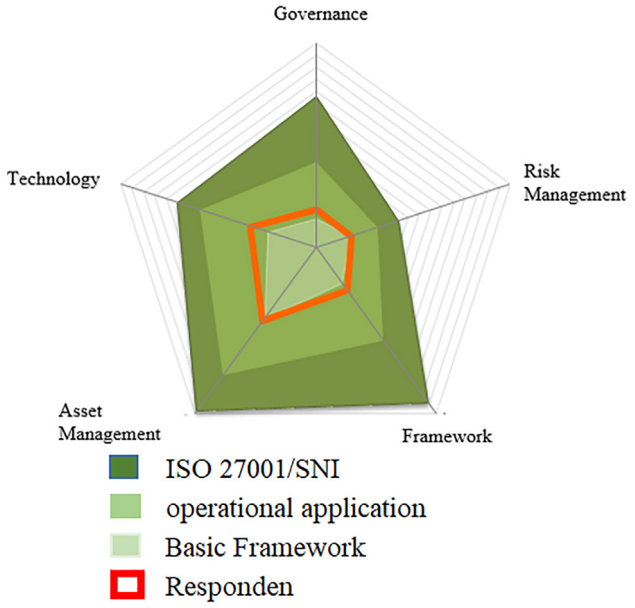

Fig. 6. Cybersecurity Gap.

Table 18
Results evaluation of the implementation of the ISO/IEC 27001:2013.

Key Factor of ISO/IEC 27001	Total Question	Score Evaluation ISO/IEC Compliance
Governance (G)	22	32
Risk Management (RM)	16	31
Framework (F)	29	44
Asset Management (AM)	38	75
Technology Aspect (TA)	26	57
Total	131	239

bination of the two analytical methods is calculated using the formula we built

$$MPS = RTS + RES \tag{4}$$

MPS: Mitigation Priority Score
RTS: Relative Threat Score
RES: Relative Evaluation Score

4.1.8. Calculating relative threat score

By using the data from the risk analysis in Fig. 3, it is obtained the number of assets that have a threat at each level of risk, where each level of risk has a weight determined in the previous risk an alysis. Then the threat score can be calculated by the following formula:

$$RTS = \frac{TS}{MTS} \tag{5}$$

RTS: *Relative Threat Score*
TS: *Threat Score*
MTS: *Maximum Threat Score*

where the threat score is the value of the weight of each threat that has an impact on assets against all levels of risk criticality.

$$TS = \sum_{i,j}^{n} AAi * RWj \tag{6}$$

Table 19
Relative threat score.

Threat	Minor (1)	Moderate (2)	Major (3)	Extreme (4)	Threat Score	Relative Threat Score
Access Leak (AL)	1	6	6	0	31	0,596
Modification (M)	1	11	1	0	26	0,500
Problem Cause by The Third party (PTP)	2	10	1	0	25	0,481
Disaster (D)	4	3	4	2	30	0,577
Destroy or temporarily lost (D/L)	3	3	5	2	32	0,615

TS	*: Threat Score*
AAi	*: Affected Assets for threat i=1 to n*
RWj	*: Risk Weight for risk level j=1 to n*

To get the Maximum threat score the writers use the formula

$$MTS = mw * tca \tag{7}$$

MTS	*: Maximum Threat Score*
mw	*: Maximum Weight of Risk level*
tca	*: Total Critical Asset*

In this case, we have 13 critical assets where the highest criticality level is extreme with a weight value of 4 so the Maximum threat score is 52 for each security threat (Table 19).

4.1.9. Calculating relative evaluation score

By using the data from the analysis of the ISO/IEC 27001 compliance evaluation (see Table. 18) the evaluation value for each section is obtained. Then the Relative evaluation score can be calculated by the following formula:

$$RES = \frac{ES}{MES} \tag{8}$$

RES	*: Relative Evaluation Score*
ES	*: Evaluation Score*
MES	*: Maximum Evaluation Score*

In evaluating the implementation of ISO/IEC 27001 compliance, each evaluation section has a different maximum evaluation score. We present the maximum evaluation score in the following Table 20.

4.1.10. Maturity level sync

To ensure the suitability between the results of the risk analysis and the value of the security index, we synchronize the maturity level of the two analysis methods. Then we construct a matrix of contributing factors for each maturity level.

Logically, the more vulnerabilities, the higher the level of risk percentage so that the lower the level of compliance with the ISO/IEC 27001 framework. On the other hand, the fewer vulnerabilities, the lower the risk level, so the higher the level of compliance with the ISO/IEC 27001 framework (see Fig. 7). Furthermore, Table 21 shows the percentage of requirements for each maturity level based on the boundary values of each dimension and threat.

Furthermore, a maturity score can be calculated which can be used as a synchronization process with the results of the analysis of the security index measurement, this is done to obtain a match between the level of risk and the value of the security index [26]

$$MST = \frac{\sum RTS}{n} 100 \tag{9}$$

MST	*: Maturity Score Threat*
RTS	*: Relative Threat Score*
n	*: Number of threat categories*

Thus, the maturity score for Threats from the results of the risk analysis was

MST	=	$\frac{\sum RTS}{n} 100$
	=	$\frac{0{,}596+0{,}500+0{,}481+0{,}577+0{,}615}{5} 100$
Maturity Level	=	55%
	=	2

To calculate the Maturity Level Security Index, it can be calculated by the following formula:

$$MSI = \frac{\sum RES}{n} 100 \tag{10}$$

Table 20
Relative evaluation score.

Dimension	Evaluation Score (ES)	Maximum Score (MS)	Relative Evaluation Score (RES)
Governance (G)	32	126	25,4
Risk Management (RM)	31	72	43,1
Framework (F)	44	159	27,7
Asset Management (AM)	75	168	44,6
Technology Aspect (TA)	57	120	47,5

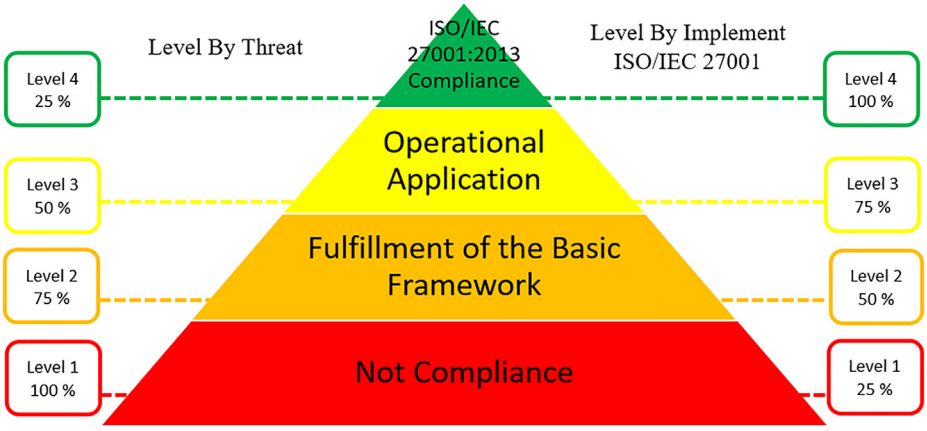

Fig. 7. Matrix Maturity Level Percentage.

Table 21
Maturity level synchronize.

Security Maturity Level Percentage		1= (25%)	2 = (50%)	3 = (75%)	4 = (100%)
Key Success factors to threat mitigation of ISO/IEC 27001 Compliance	G	(5%)	(10%)	(15%)	(20%)
	RM	(3%)	(6%)	(8%)	(11%)
	F	(6%)	(12%)	(18%)	(25%)
	AM	(7%)	(13%)	(20%)	(26%)
	TA	(5%)	(9%)	(14%)	(19%)
Contribution to Success Mitigation Risk base on Threat	AL	(20%)	(15%)	(10%)	(5%)
	M	(20%)	(15%)	(10%)	(5%)
	PTP	(20%)	(15%)	(10%)	(5%)
	D	(20%)	(15%)	(10%)	(5%)
	D/L	(20%)	(15%)	(10%)	(5%)
Threat Maturity Level Percentage		1 = (100%)	2 = (75%)	3 = (50%)	4 = (25%)

MSI	*: Maturity Security Index*
RES	*: Relative Evaluation Score*
n	*: Number of threat parts ISO/IEC 27001*

Thus, the security index maturity value for the results of the ISO/IEC 27001 framework compliance evaluation analysis was

$$MSI = \frac{\sum RES}{n} 100$$
$$= \frac{25{,}40+43{,}06+27{,}67+44{,}64+47{,}50}{5} 100$$
$$Maturity\ Level = 37{,}65\%$$
$$= 2$$

After knowing that the Maturity score threat is 55% and the maturity score index is 37.65%, then based on the maturity matrix table (see Table 21) it can be seen that the maturity level of the results of these two analytical methods is 2, namely the "basic framework" where the percentage level of achievement of the security index <50% and the risk level <75%, so it can be said that the results of the combination of these two analytical methods are synchronous.

Furthermore, after getting the two variables to calculate the Mitigation Priority Score with equation (4), the results are obtained in Table 22.

Mitigation priority is determined based on the order of the highest Mitigation priority score for each part of ISO/IEC 27001 against each existing threat. The highest Mitigation Priority score gets the first priority mitigation (P1), which means that the recommendation labeled P1 becomes the main priority for the organization, the lowest mitigation priority score gets the mitigation priority 5 (P5), which means that the recommendation with the P5 label becomes the lowest or final mitigation priority for carried out by the organization.

4.2. Implementation recommendation

Table 23 shows 29 security recommendations and their priorities based on the key to success in achieving ISO/IEC 27001 compliance and the security threats faced by the organization. Implementation of recommendations is the stage of designing and implementing information technology security recommendations that have been proposed to the company. Recommendations that will be implemented are recommendations that have been determined by the company to be implemented (see Table 24).

4.2.1. Designing IT Policy (Project Code: ITG)

It is a policy design that contains information technology governance rules that exist in the company. The design involves all departments that have a correlation with business processes and the legality of IT policies on the use of information technology in the company (Fig. 8).

IT policy is at the second level under the corporate policy, IT policy is legalized at the board of directors' level and becomes a guide in building SOPs for IT management and operations in the company. We build 23 IT Policies that involve cross-departmental (Table 25).

4.2.2. Designing infrastructure and systems based on High Availability (Project Code: IF)

Infrastructure and Systems based on High Availability are infrastructures built by eliminating the possibility of a loss of resource function due to the system or device failures. The company approved the procurement of IT infrastructure and system development projects based on HA (Fig. 9).

There are several needs related to the development of infrastructure and systems based on HA (Table 26).

Firewall Sophos XG230, is used as a security device at layers 2 and 3, besides that this device is also used as a traffic controller

Table 22
Mitigation priority score and mitigation priority.

ISO/IEC 27001 Dimension	Relative Evaluation Score	Threat	Relative Threat Score	Mitigation Priority Score	Mitigation Priority
Governance	0,25	*AL*	0,60	0,85	P2
		M	0,50	0,75	P4
		PTP	0,48	0,73	P5
		D	0,58	0,83	P3
		D/L	0,62	0,87	P1
Risk Management	0,43	*AL*	0,60	1,03	P2
		M	0,50	0,93	P4
		PTP	0,48	0,91	P5
		D	0,58	1,01	P3
		D/L	0,62	1,05	P1
Framework	0,28	*AL*	0,60	0,87	P2
		M	0,50	0,78	P4
		PTP	0,48	0,76	P5
		D	0,58	0,85	P3
		D/L	0,62	0,89	P1
Asset Management	0,45	*AL*	0,60	1,04	P2
		M	0,50	0,95	P4
		PTP	0,48	0,93	P5
		D	0,58	1,02	P3
		D/L	0,62	1,06	P1
Technology Aspect	0,48	*AL*	0,60	1,07	P2
		M	0,50	0,98	P4
		PTP	0,48	0,96	P5
		D	0,58	1,05	P3
		D/L	0,62	1,09	P1

Where AL = Access Leak, M = Modification, PTP = Problem Cause by The Third-party, D = Disaster, and D/L = Destroy or temporarily lost.

Table 23
Executive report cybersecurity recommendation with mitigation targets.

No	*ISO/IEC* 27001 *Category*	*Mitigation Solutions*	*Threat Mitigation Targets*	*Asset Targets*	*Priority*
1	G	IT Policy	All Risks	All Assets	P1
2		Standard Operating Procedure	All Risks	All Assets	P1
3	RM	Risk Assessment Framework	All Risks	All Assets	P1
4		Business Impact Analysis Framework	All Risks	All Assets	P1
5		Business Continuity Plan	Disaster	All Assets	P3
6	F	Disaster Recovery Plan	Disaster	All Assets	P3
7		Documentation	Modification	All Assets	P4
8		Analysis Method	All Risks	All Assets	P1
9	AM	Data Warehouse Management	Destroy or temporarily lost	All Hardware	P1
10		Procurement Planning	Destroy or temporarily lost	All Hardware	P1
11		Distribution Planning	Destroy or temporarily lost	All Hardware	P1
12		Removal Planning	Destroy or temporarily lost	All Hardware	P1
13	TA	Disaster Recovery Centre	Disaster	All Assets	P3
14		High Availability System	Destroy or temporarily lost	Database System	P1
15		High Availability Infrastructure	Destroy or temporarily lost	All Hardware	P1
16		Email Security Gateway	Access Leak, Problem caused by the third party	Email System	P1
17		Identity Access Management System	Access Leak	Information Access Server	P2
18		Intrusion Detection System	Access Leak	Information Access Server	P2
19		Vulnerability Management System	Access Leak, Problem caused by the third party	Information Access Server	P1
20		Compliance Management System	Access Leak, Problem caused by the third party	Information Access Server	P1
21		Policy and procedure management tools	Access Leak, Problem caused by the third party	Information Access Server	P1
22		Network Time Protocol System	Modification	All System	P4
23		Logging System	Modification	All System	P4
24		Management DNS	Modification	All System	P4
25		Antivirus Server	The Problem caused by the third party	All System	P5
26		IT Risk management tools	Destroy or temporarily lost	All Assets	P1
27		Digital Form Record system	Modification	All Assets	P4
28		Backup and restore management system	Destroy or temporarily lost	All Systems	P1
29		Monitoring System	Modification	All Assets	P4

on the network. 2 units are allocated for the main data center and 1 unit for DRC. This device has an Auto Failover feature so that the presence of 2 units of this device can guarantee the availability of the device in the event of a failure on one of the devices. Switch 10g Edge-Core ESC5520-18X and Switch Edge-Core 1g Edge-Core ESC4510-28T are network devices that function as links between data center devices. The HP ProLiant DL380 G10 server is a physical server that is used as a hypervisor host for Virtual servers. ESXi Hypervisor is an engine for server virtualization technology based on VMWare vSphere. This software is installed on each physical

server. vCenter Server is a centralized management utility for VMware and is used to manage virtual machines, multiple ESXi hosts, and all dependent components from one central location. This software also organizes ESXi hosts into a HA cluster so that each ESXi host can replace the function of the failed host. VMware Virtual SAN is a very simple storage solution optimized for virtual environments that brings an application-centric approach to storage management. VMware Site Recovery Manager (SRM) is a software integrated with replication technology to provide policy-based management, automated Disaster Recovery Plan settings to reduce downtime in the event of a disaster and to perform non-disruptive testing of Disaster Recovery Plans. Oracle Data Guard functions as a replacement for the production database when the production database suddenly becomes unusable/dead (Fig. 10).

Table 24
Approved recommendations.

No	Recommendation Approved	Project Code
1	IT Policy	ITG
2	High Availability Infrastructure	IF
3	High Availability System	IF
4	Intrusion Detection System	SP
5	File Integrity Manager	SP
6	Compliance Management System	SP
7	Policy and procedure management tools	SP
8	Logging System	SP
9	Vulnerability Management System	SP
10	Identity Access Management System	SP
11	Email Security Gateway	SP

4.2.3. Designing Security Platform (Project Code: SP)

Security Platform is a system that functions to mitigate and handle security problems. Below is a security platform architecture that was built to mitigate and handle system security problems. Below is the architecture of the security system that was built:

There are 4 servers built as a security platform with the following specifications (Table 27):

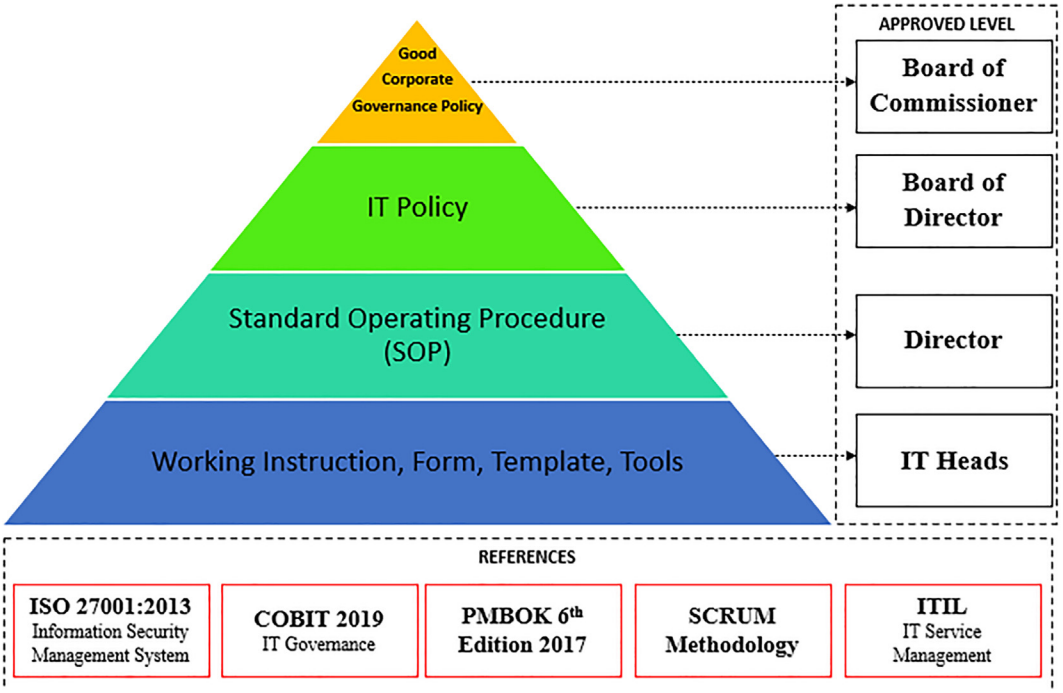

Fig. 8. Information Technology Policy and Business Process Hierarchy.

Table 25
IT policy list example.

No	Policy Name
1	**IT System Acquisition** is a policy that regulates the selection, selection, and establishment of new IT systems, as well as initiation of development of existing IT systems
2	**Account and Password** is a policy that regulates the standard of accounts and passwords in the Company
3	**Production Environment Control** is a policy that regulates the conditions of the production environment in the Company
4	**IT System Change** is a policy that regulates changes (change management) to the Company's IT System
5	**Access Control** is a policy that regulates the standardization of access rights, requests, grants, uses, and evaluations of access rights
6	**Backup & restore** is a policy that regulates backup and restores activities on Company systems, data, and information
7	**Partner Management** is a policy that regulates the relationship between IT Erajaya with partners or partners or third parties who carry out IT-related work in the Company.
8	**IT Data & Information** is a policy that regulates the classification of data and information, storage, and distribution of Company-owned information
9	**Viruses, Spam, and Malware** is a policy that regulates the handling and prevention of viruses, spam, and malware on IT resources owned by the Company
10	**Disaster Recovery Plan** is a policy that regulates disaster management standards that have an impact on IT operations
11	**IT Risk** is a policy that regulates IT risk management in the Company

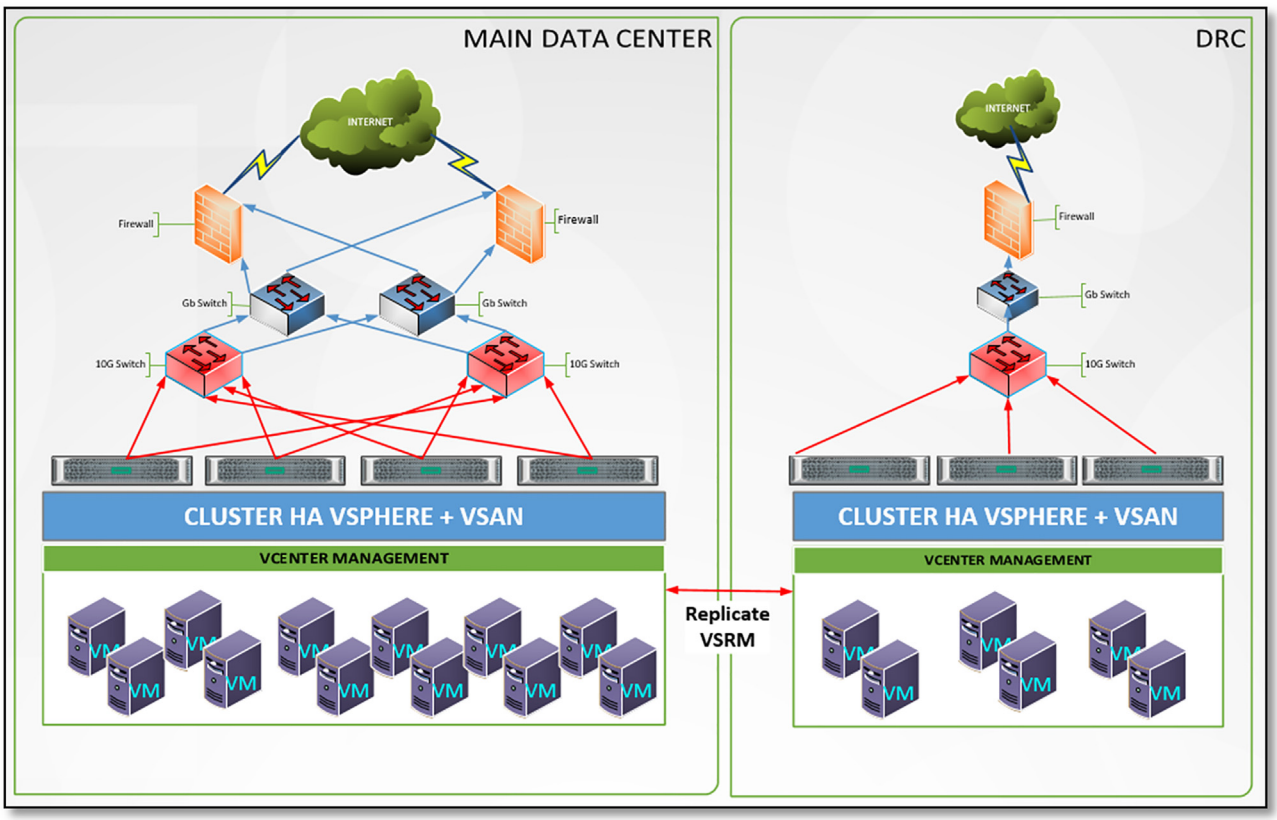

Fig. 9. Topology Infrastructure HA.

Table 26
Infrastructure Requirement.

No	Category	Requirement	Qty
1	Hardware	Firewall Sophos XG230	3
2		Switch Edge-Core 10G ESC5520-18X	2
3		Switch Edge-Core 1 Gb ESC4510-28 T	2
4		Server HP ProLiant DL380 G10	4
5	Software	VMWare ESXi Hypervisor	7
6		VCenter Server	2
7		VMWare VSAN	2
8		VMWare VSRM	1
9		Oracle Data Guard	1

All in One Security Platform
This server has several features, namely

a. Intrusion Detection System functions as detection of security attacks that occur in the entire system and provides warnings to system security officers.
b. File Integrity Manager functions as monitoring the integrity of the configuration document on the entire server.
c. Compliance Management System which functions as a server configuration detection system for cybersecurity compliance such as PCI-DSS, NIST 800-53, GDPR, TSC, and HIPAA
d. Policy and Procedure Management which functions as a server configuration detection against the CIS benchmark hardening standard and provides recommendations for corrective steps that need to be taken.
e. Logging System which functions as a management logging system, log data can be used as an analysis of activity and situation that is currently happening on the server.

Vulnerability Management System
This server is used as a vulnerability assessment of all servers in the data center. With this server, the vulnerabilities contained in the server can be identified for the patching process (closing the security gap).

Identity Access Management
This server is used to manage access rights based on authentication, authorization, and user accounting for servers in the datacenter centrally. The settings include a user access matrix and a security access matrix so that control over user access can be properly monitored and managed.

Email Security Gateway
A server device that functions as a gateway for the email system, so that every inbound and outbound email traffic will be filtered on this device.

4.3. Testing result of implementation recommendation

The writers test by trying to send cybersecurity attacks directly to the target company's systems and applications to ensure the implementation of the selected security recommendations can overcome and mitigate security attacks and threats (Table 28).

4.4. Evaluation result of implementation recommendation

Evaluation is the stage of quantitative analysis of the results of the implementation of security recommendations that have been built. The evaluation aims to find out whether there are differences before and after the implementation of security recommendations. In the calculation process at the evaluation stage, we use programming with R language with a value of Degree of freedom (df) = 0.05

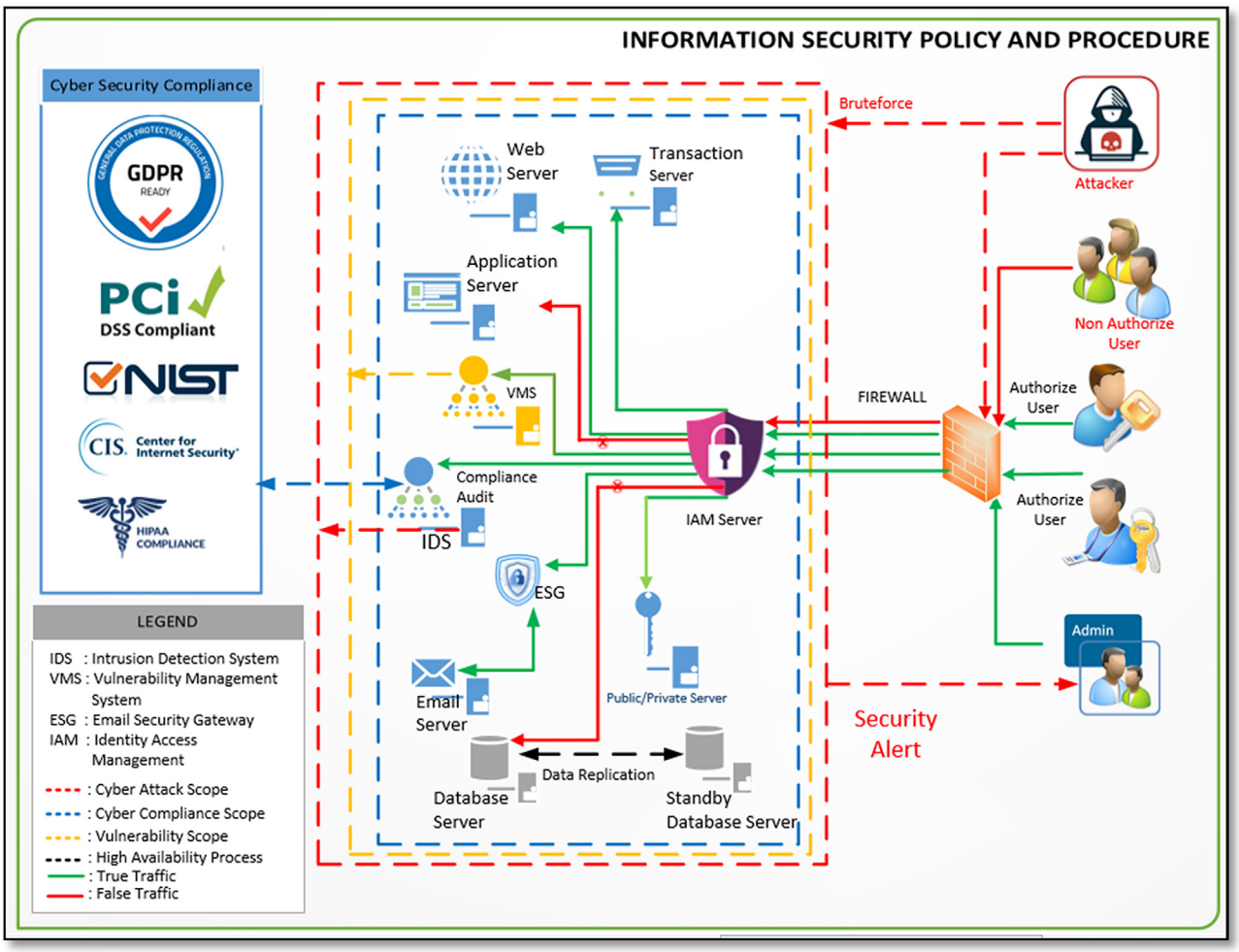

Fig. 10. Architecture Security Platform.

Table 27
Server specification.

No	Component	All in One Security Platform	Vulnerability Management System	Identity Access Management	Email Security Gateway
1	**vCPU**	4 Core	4 Core	4 Core	Min 1 Core, Max 4 Core
2	**RAM**	8 GB	8 GB	8 GB	Min 32 GB, Max 2 TB
3	**HDD**	200 GB	100 GB	100 GB	Min 32 GB, Max 2 TB
4	**OS**	Ubuntu Server 20	Ubuntu Server 20	Linux Centos 8	Fortinet
5	**Apps**	Wazuh	Nessus Pro, Arachni	FreeIPA	Fortimail

(5%). Provisions for the selection of statistical analysis methods in conducting evaluations (Fig. 11).

Evaluation data collection is done by distributing questionnaires that have been given a weighted value to respondents who have a relationship with company assets related to the success of security recommendations against threats and security attacks that exist in the company based on test data from the results of the implementation of the recommendations (Table 29).

To gain the best results, we validate the questionnaire data before it is distributed to respondents. The validation of the questionnaire data was carried out using the expert judgment method by conducting interviews with experts. The results of the validation of the questionnaire data are valid for collecting evaluation data. Next, we build 3 hypotheses based on the research problem, namely:

Table 28
Testing result.

No	Testing Method	Result
1	Brute force	Success to detect and blocked
2	Email Phishing with Link	Success to detect and blocked
3	Email Phishing with Malware and Virus	Success to detect and blocked
4	Modification File Configuration	Success to detect
5	Power Supply Redundancy	Success to Failover
6	Network Adapter VSAN Redundancy	Success to Failover
7	Vulnerability Finding	Success in finding vulnerability on the system
8	Security Configuration Compliance	Success to finding miss-configuration

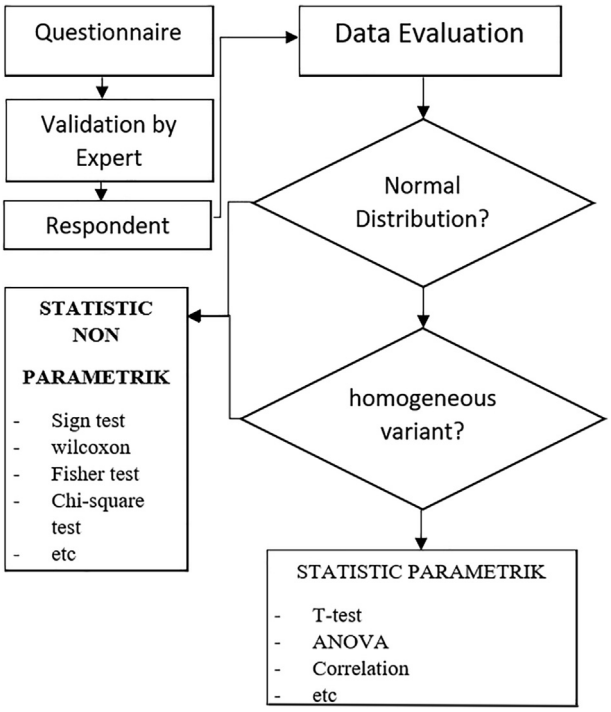

Fig. 11. Statistical Approach.

Table 29
Respondent criteria.

No	Respondent Criteria
1	Has a function that is directly responsible for the asset object
2	Has a function on the use of asset objects
3	Has a function for the operational continuity of the asset object
4	Has a corporate regulatory compliance function related to asset management

Hypothesis 1

H_0: There is no significant effect between threats to information technology security systems that implement and do not implement information technology security system recommendations on the value of the ISO/IEC 27001 compliance evaluation index.

H_A: There is a significant influence between threats to information technology security systems that implement and do not implement information technology security system recommendations on the value of the ISO/IEC 27001 compliance evaluation index.

The data used in hypothesis test 1 is the result of the evaluation of the implementation of the ISO/IEC 27001 framework in the organization to the conditions before and after the implementation of information technology security system recommendations. Plotting the data on the two evaluation results shows an increase in the evaluation value of the implementation of the ISO/IEC 27001 framework in the organization (see Fig. 12).

Based on Fig. 12, to determine the significant level of difference between the two conditions of information technology security systems in organizations, hypothesis 1 was tested using a parametric statistical approach with the Paired *t*-test method. This method has 2 conditions, namely, the data population must be normally distributed and have the same homogeneity. The first condition can be determined by performing a normality test, we use the Shapiro Wilk test method with the formula [27].

$$W = \frac{\left(\sum_{i=1}^{n} a_i y_{(i)}\right)^2}{\sum_{t=1}^{n}\left(x_i - \bar{y}\right)^{2'}} \tag{11}$$

Where $y_{(i)}$ *is the* i^{th} *order statistic,* $\bar{y}$ is the sample mean, and a_i constants obtained:

$a_i = (a_1, \cdots, a_n) = \frac{m^T V^{-1}}{(m^T V^{-1} V^{-1} m)^{1/2}}$, where m = (m1, . . . , mn) T are the expected values of the order statistics of independent and identically distributed random variables sampled from the standard normal distribution and V is the covariance matrix of those order statistics.

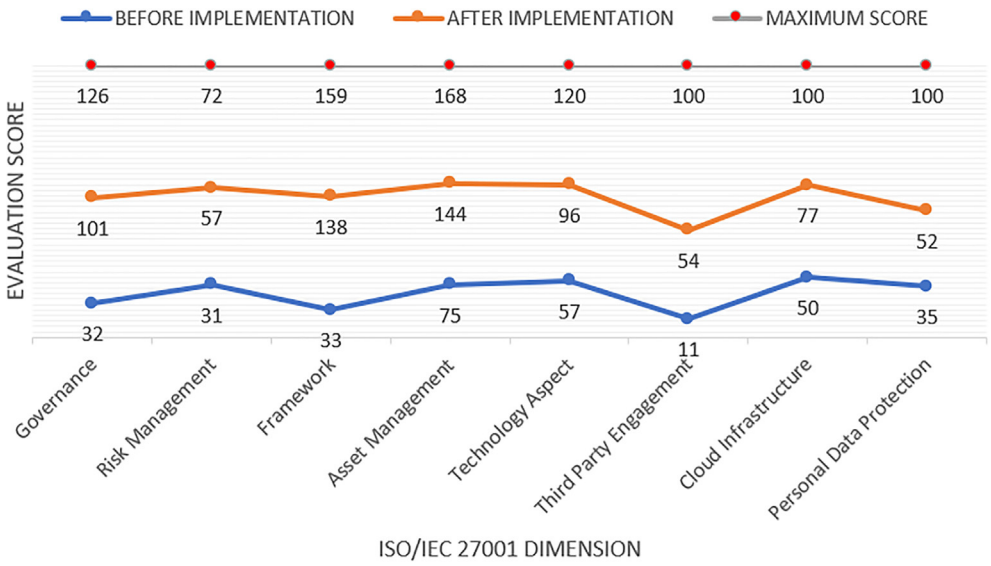

Fig. 12. Evaluation Score ISO/IEC 27001 Compliance.

In statistics plot, Q-Q (quantiles) plays a very important role in graphically analyzing and comparing two probability distributions by plotting their quantiles against each other. If the two distributions we are comparing are the same, then the points on the Q-Q plot lie perfectly on the straight-line y = x. Visually (see Fig. 13) shows the data distribution of the two populations is normally distributed but not perfect. Each data in the population is getting closer to the line y = x.

With a significant level value of = 5% (0.05), a distribution is said to be normal if the significance level is > 0.05, whereas if the significance level is < 0.05 then the distribution is said to be abnormal. Furthermore, with the Shapiro Wilk test method, it is known that the population data before implementation has a p-Value of 0.6469 and after implementation has a p-Value of 0.2037 so that both p-Value values > 0.05, it can be concluded that the data is normally distributed.

Furthermore, the second requirement in the parametric statistical approach is that the data population must have the same variance. The level of significant homogeneity of the data can be determined by using Levene's test method with the formula [28]

$$W = \frac{N-k}{k-1}\frac{\sum_{i=1}^{k} N_i (Z_i - Z..)^2}{\sum_{i=1}^{k}\sum_{j=1}^{N_i} (Z_{ij} - Z_{i.})^2} \tag{12}$$

k is the number of different groups to which the sampled cases belong,

N_i is the number of cases in the i th group

N is the total number of cases in all groups

Y_{ij} is the value of the measured variable for the jth case from the ith group,

$$Z_{ij} = \begin{cases} \left|Y_{ij} - \bar{Y}_i\right|, \bar{Y}_i \text{ is mean of the } i-th \text{ group}, \\ \left|Y_{ij} - \tilde{Y}_i\right|, \tilde{Y}_i \text{is median of the } i-th \text{ group} \end{cases}$$

Homogeneous test interpretation can be seen through the significant value. If the value is significant/p-Value > 0.05 then the data can be said to be homogeneous. By using Levene's test method in equation (14) with the evaluation value variable and the status of the recommendation implementation, it is obtained that the value of F count = 3.8084 so that by looking at the F distribution table with a significance level of 5% or 0.05, the p-Value value of the variance test is 0.0713. So, because the p-value > 0.05, it can be concluded that the population data have the same variance

After the two conditions are met, the parametric statistical test using the paired t-test method can be carried out with the formula [29]

$$t = \frac{\bar{D}}{S_D \,/\, \sqrt{n}} \tag{13}$$

$\bar{D}$ = Mean of the difference score = $\bar{X}_2 - \bar{X}_1$

S_D = SD of the difference scores = $\sqrt{s_1^2 + s_2^2 - 2r_{12}s_1s_2}$

n = Number of pairs; SD divided by $\sqrt{n}$ = Standard Error of the difference score

Because both conditions have been met, the Paired t-test on the data population can be carried out. The results of the significant test with the paired t-test method (15) obtained p-value = 0.002 138 < 0.05 so it can be concluded that the null-hypothesis is rejected, which means that there is a significant influence between threats to information technology security systems that implement and do not implement recommendations for information technology security systems on the value of the ISO/IEC 27001 compliance evaluation index.

Hypothesis 2

H_0: There is no association relationship between threats to information technology security systems that apply recommendations and do not apply recommendations to the level of criticality of information technology security threats.

H_A: There is an association relationship between threats to information technology security systems that apply recommendations and do not apply recommendations to the level of criticality of information technology security threats.

The data in hypothesis test 2 is data obtained from respondents' answers to a questionnaire consisting of 12 examples of threats that exist in the organization's information technology security system. The answer to the questionnaire has an objective to assess the criticality level of a security system threat to the organization's assets and business against the mitigation steps taken. The data consists of 2 populations, namely the population of the threat criticality level data before implementation and after implementation (see Fig. 14).

Based on the visual plotting of the two populations' data (see Fig. 14) there is a decrease in the criticality level of threats to conditions before and after the implementation of security system recommendations. Prior to the implementation of the security recommendations, threats with extreme and major criticality levels were found, while after the implementation of the security system recommendations, they were not found again. To get a significant value for the changes in these conditions, hypothesis 2 was tested using a non-parametric statistical approach using Pearson's chi-square t-test method, this approach was chosen because the requirements for the parametric statistical approach were not met. Pearson's chi-square t-test has the formula [27]

$$x^2 = \sum_{i=1}^{n} \frac{(Oi - Ei)^2}{Ei} = N\sum_{i=1}^{n} \frac{\left(\frac{O_i}{N} - p_i\right)^2}{E_i} \tag{14}$$

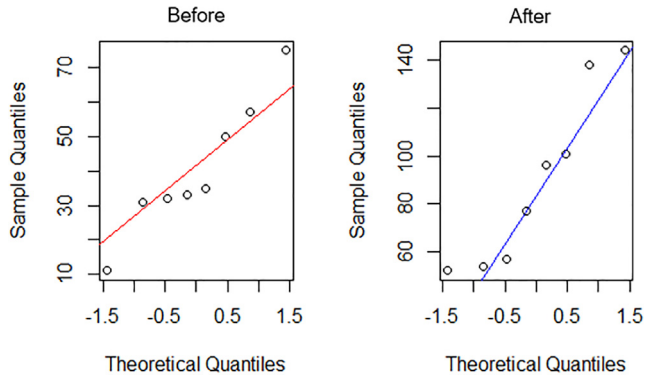

Fig. 13. Plotting Quantiles.

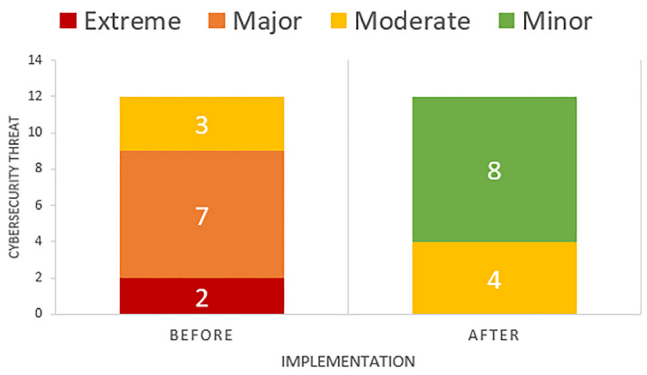

Fig. 14. Criticality threat before and after implementation recommendation.

x^2 Pearson's cumulative test statistic, which asymptotically approaches a x^2 distribution.

O_i the number of observations of type i

N total number of observations

E_iNp_i = the expected (theoretical) count of type i, asserted by the null hypothesis that the fraction of type i in the population is p_i

n the number of cells in the table.

Based on the results of the hypothesis test using the Pearson's chi-squared (14) method, the p-value was 0.0006605 < 0.05, which means the null hypothesis was rejected. P-Value on Pearson's chi-squared test may be wrong because the resulting accuracy is not so good. This is the shortcoming of the non-parametric statistical approach so that validation of the accuracy of significant values is needed by using the Fisher test method with equation (15) [30]

$$p = \frac{(a+b)!(c+d)!(a+c)!(b+d)!}{a!b!c!d!n!} \quad (15)$$

p = p-value

a, b, c, d = value in a contingency table

n = total frequency

With the fisher test method obtained p-Value 0.00008284 < 0.05. So based on the p-value results in the Pearson's chi-square test and the p-value Fisher test results show that both results are p-Value < 0.05 so it can be concluded that there is an association relationship between threats to information technology security systems that apply the recommendations and do not implement the recommendations on the level of criticality of information technology security threats.

Hypothesis 3

H_0: There is no association relationship between systems that implement and do not implement recommendations based on ISO/IEC 27001 for cybersecurity attack mitigation.

H_A: There is an association relationship between systems that implement and do not implement recommendations based on ISO/IEC 27001 for cybersecurity attack mitigation.

The data on hypothesis test 3 is the data obtained from the total answers of each respondent to the 12 questionnaires. The answers to the questionnaire have an objective to assess the association relationship between the effectiveness of mitigation measures based on the ISO/IEC 27001 framework after the implementation of information technology security system recommendations against cyber security attacks. Plotting population data shows an increase in the value of the effectiveness of the mitigation carried out against cybersecurity attacks (see Fig. 15).

To determine the significant level of association relationship between increasing the effectiveness of threat mitigation based on the ISO/IEC 27001 framework against cybersecurity attacks, hypothesis 3 was tested using a non-parametric statistical approach using the Pearson's chi-square t-test method. not fulfilled. The results of hypothesis testing using Pearson's chi-squared method obtained p-Value 000005221 < 0.05, which means the null hypothesis is rejected. The p-Value value in Pearson's chi-squared test may be wrong, so validation is needed using the Fisher test method, the p-Value value is 0.00000005658 < 0.05, which means the null hypothesis is rejected. So based on the two results, p-Value < 0.05, it can be concluded that there is an association relationship between systems that implement and do not implement recommendations based on ISO/IEC 27001 for cybersecurity attack mitigation.

5. Conclusions

Threats and attacks on information technology security systems have increased very significantly. Companies need to carry out risk management and evaluate the readiness of information security systems to minimize the level of security risk and provide guarantees for business continuity. With risk analysis and cybersecurity compliance evaluation, it can be seen the level of risk of each threat and security gap that exists in the company. Risk analysis and evaluation of cybersecurity compliance can assist companies in making policies to develop information technology security systems effectively and efficiently. Based on the research that we have conducted on companies engaged in the retail industry, it shows that the proposed model can provide effective results in mitigating security threats and proves that there is a relationship between risk and the value of cybersecurity compliance evaluations against security threats. This is evident from the results of the evaluation with a statistical approach showing an increase in the average value of the evaluation of ISO/IEC 27001 compliance from 36.27 to 82.37 with the p-value of Paired T-Test is 0.002138 < 0.05, meaning that there is a significant influence between threats to the security of the information system technology that implements and does not apply information technology security system recom-

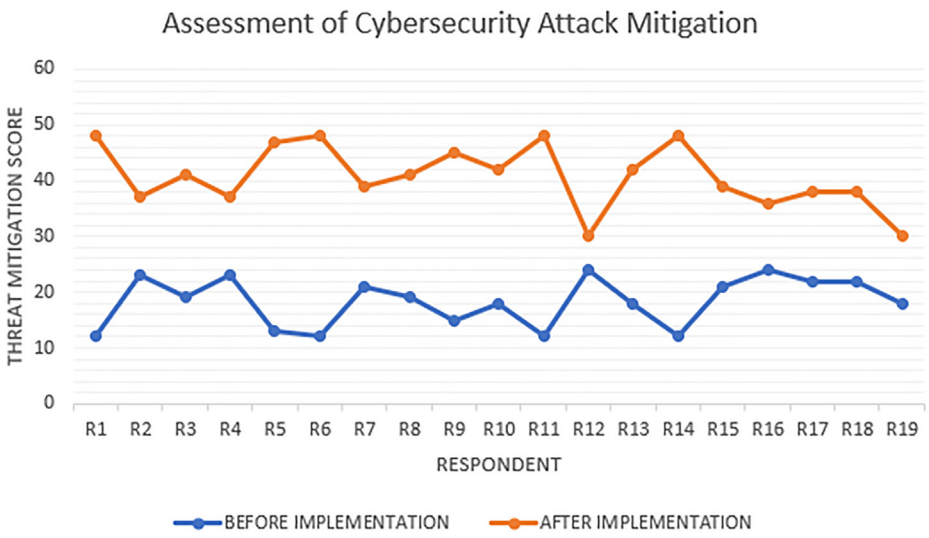

Fig. 15. Mitigation Cybersecurity Attack.

mendations to the ISO/IEC 27001 compliance evaluation index value. Furthermore, based on 12 types of threat samples, it shows a decrease in the average threat criticality level from 8.75 to 4.00 with a p-value the chi-square test is 0.0006605 < 0.05 and the Fisher Test p-value is 0.000008284 < 0.05, meaning that there is an association relationship between threats to information technology security systems that apply recommendations and do not apply recommendations to the criticality level of information technology security threats. While the results of the evaluation of the relationship between the implementation of security system recommendations on cybersecurity attack mitigation showed an increase in the effectiveness of cyber-attack mitigation from an average rating of 18.32 to 40.74 with the p-value of the chi-square test being 0.000005221 < 0.05 and the Fisher Test being 0.00000005658 < 0.05 means that there is an association relationship between systems that implement and do not implement recommendations based on ISO/IEC 27001 for cybersecurity attack mitigation.

Security threats will continue to grow along with advances in information technology. Business infrastructure has also begun to be dominated by cloud-based infrastructure. This research has a weakness, where the analysis does not involve the enterprise resource planning application and surrounding application which is the main system of the company's business operations. The vulnerability of business operational applications can create threats that trigger security breaches. In mitigating cybersecurity threats, many things need to be proven and analyzed. One of the next works is the development of the proposed method by considering the security control based on the Open Web Application Security Project (OWASP) on the enterprise resource planning application and surrounding application as one of the important aspects in mitigating cyber security attacks. In addition, this study does not analyze the impact of implementing information technology policies on employee work patterns in mitigating security threats. This is a follow-up work to assess the level of security awareness of the application of information technology policies to the level of cybersecurity threat risk.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The writers would like to thank the contributions of all dedicated Departments for their valuable efforts in building the technology and information security system. This security system would not be possible to build without their invaluable involvement.

References

[1] I. Goddijn, 2020 Q3 Report Data Breach QuickView 3308 W Clay St, Richmond, VA 23230, United States, Oct. 2020. Accessed: Mar. 15, 2021. [Online]. Available: https://pages.riskbasedsecurity.com/en/en/2020-q3-data-breach-quickview-report-0.

[2] M. Henriquez, The top 10 data breaches of 2020, https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020, Dec. 03, 2020. https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020 (accessed Feb. 15, 2021).

[3] E. Y. Yildirim, The importance of risk management in information security, *Int. J. Adv. Electron. Comput. Sci.*, 4(1) (2017) 18–21, [Online]. Available: http://iraj.in.

[4] Kure HI, Islam S, Razzaque MA. An integrated cyber security risk management approach for a cyber-physical system. Appl. Sci. (Switzerland) 2018;8(6):1–29. doi: https://doi.org/10.3390/app8060898.

[5] M. Frayssinet Delgado, D. Esenarro, F. F. Juárez Regalado, M. Díaz Reátegui, Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations, *3C TIC: Cuadernos de desarrollo aplicados a las TIC*, 10(2) (2021) 123–141, doi: 10.17993/3ctic.2021.102.123-141.

[6] Diesch R, Pfaff M, Krcmar H. A comprehensive model of information security factors for decision-makers. Comput. Secur. 2020;92:101747.

[7] G. Roldán-Molina, M. Almache-Cueva, I. Yevseyeva, C. Silva-Rabadão, V. Basto-Fernandes, A decision support system for corporations cybersecurity management, (2017). doi: 10.23919/CISTI.2017.7975826.

[8] Fielder A, Panaousis E, Malacaria P, Hankin C, Smeraldi F. Decision support approaches for cyber security investment. Decis. Support. Syst. 2016;86:13–23. doi: https://doi.org/10.1016/j.dss.2016.02.012.

[9] M'manga A, Faily S, McAlaney J, Williams C, Kadobayashi Y, Miyamoto D. A normative decision-making model for cyber security. ICS 2019;27(5):636–46.

[10] Paul JA, Zhang M. Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker. Eur. J. Oper. Res. 2021;291(1):349–64. doi: https://doi.org/10.1016/j.ejor.2020.09.013.

[11] D. Achmadi, Y. Suryanto, K. Ramli, On developing information security management system (ISMS) Framework for ISO 27001-based Data Center, (2018).

[12] M. Tamimi, A. Alzahrani, R. Aljohani, M. Alshahrani, B. Alharbi, Security review based on ISO 27000/ ISO 27001/ISO 27002 STANDARDS: A case study research, 2019. [Online]. Available: http://iraj.in.

[13] Syreyshchikova NV, Pimenov DY, Mikolajczyk T, Moldovan L. Information safety process development according to ISO 27001 for an industrial enterprise. Procedia Manuf 2019;32:278–85. doi: https://doi.org/10.1016/j.promfg.2019.02.215.

[14] Culot G, Nassimbeni G, Podrecca M, Sartor M. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. TQM 2021;33(7):76–105.

[15] A. Tewari, Comparison between ISO 27005, OCTAVE & NIST SP 800-30, *sisainfosec.com*, 2020. Comparison between ISO 27005, OCTAVE & NIST SP 800-30 (accessed Mar. 10, 2021).

[16] Irena Gutandjala I, Gui A, Maryam S, Mariani V. Information system risk assessment and management (Study Case at XYZ University). In: 2019 International Conference on Information Management and Technology (ICIMTech), Sep. p. 6022–607.

[17] Ganin AA, Quach P, Panwar M, Collier ZA, Keisler JM, Marchese D, et al. Multicriteria decision framework for cybersecurity risk assessment and management. Risk Anal. 2020;40(1):183–99.

[18] Gourisetti SNG, Mylrea M, Patangia H. Cybersecurity Vulnerability Mitigation Framework through Empirical Paradigm (CyFEr): Prioritized Gap Analysis. IEEE Syst J Jun. 2020;14(2):1897–908. doi: https://doi.org/10.1109/JSYST.2019.2913141.

[19] Sensuse DI, Syarif M, Suprapto H, Wirawan R, Satria D, Normandia Y. Information security evaluation using KAMI index for security improvement in BMKG. In: *2017 5th International Conference on Cyber and IT Service Management (CITSM)*. p. 1–4. doi: https://doi.org/10.1109/CITSM.2017.8089293.

[20] V. Monev, Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002, 2020.

[21] S. Yulianto, C. Lim, B. Soewito, Information Security Maturity Model A Best Practice Driven Approach to PCI DSS Compliance, 2016.

[22] K. Razikin, A. Widodo, General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance," 2021.

[23] Hamdi Z, Anir Norman A, Nuha Abdul Molok N, Hassandoust F. A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors. *J Phys Conf Ser*, Dec. 2019;1339(1):012103.

[24] checkpoint.com, What is a Cyber Attack?, *checkpoint.com*, 2021. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/ (accessed Feb. 15, 2021).

[25] Lewis WE. PDCA/Test: A Quality Tool Framework for Software Testing. Texas: Auerbach Publishers; 1999.

[26] Umar R, Riadi I, Handoyo E. Analysis security of SIA based DSS05 on COBIT 5 using capability maturity model integration (CMMI). Sci. J. Inf. 2019;6(2):193–202. doi: https://doi.org/10.15294/sji.v6i2.17387.

[27] J. Arnastauskaitė, T. Ruzgas, M. Bražėnas, An exhaustive power comparison of normality tests, *Mathematics*, 9(7) 2021, doi: 10.3390/math9070788.

[28] M. Yunus Shukor, Bartlett and the Levene's tests of homoscedasticity of the modified Gompertz model used in fitting of Burkholderia sp. strain Neni-11 growth on acrylamide, *Bioremed. Sci. Technol. Res.*, 4(1) (2016) 18–19 [Online]. Available: http://journal.hibiscuspublisher.com/index.php/BSTR.

[29] Rietveld T, van Hout R. The paired t test and beyond: Recommendations for testing the central tendencies of two paired samples in research on speech, language and hearing pathology. J. Commun. Disord. 2017;69:44–57. doi: https://doi.org/10.1016/j.jcomdis.2017.07.002.

[30] Kim H-Y. Statistical notes for clinical researchers: Chi-squared test and Fisher's exact test. Restorative Dentist. Endodont. 2017;42(2):152. doi: https://doi.org/10.5395/rde.2017.42.2.152.