risks

MDPI

Article

Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools

Nungky Awang Chandra [1], Kalamullah Ramli [1,*], Anak Agung Putri Ratna [1] and Teddy Surya Gunawan [2]

[1] Electrical Engineering, The University of Indonesia, Depok 16424, Indonesia
[2] Electrical and Computer Engineering Department, Kulliyyah of Engineering, International Islamic University Malaysia, P.O. Box 10, Kuala Lumpur 50728, Malaysia
* Correspondence: kalamullah.ramli@ui.ac.id

Abstract: This paper describes the development of situational awareness models and applications to assess cybersecurity risks based on Annex ISO 27001:2013. The risk assessment method used is the direct testing method, namely audit, exercise and penetration testing. The risk assessment of this study is classified into three levels, namely high, medium and low. A high-risk value is an unacceptable risk value. Meanwhile, low and medium risk values can be categorized as acceptable risk values. The results of a network security case study with security performance index indicators based on the percentage of compliance with ISO 27001:2013 annex controls and the value of the risk level of the findings of the three test methods showed that testing with the audit method was 38.29% with a moderate and high-risk level. While the test results with the tabletop exercise method are 75% with low and moderate risk levels. On the other hand, the results with the penetration test method are 16.66%, with moderate and high-risk levels. Test results with unacceptable risk values or high-risk corrective actions are taken through an application. Finally, corrective actions have been verified to prove there is an increase in cyber resilience and security.

Keywords: situational awareness; audit; exercise; penetration test; risk

Citation: Chandra, Nungky Awang, Kalamullah Ramli, Anak Agung Putri Ratna, and Teddy Surya Gunawan. 2022. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. *Risks* 10: 165. https://doi.org/10.3390/risks10080165

Academic Editor: Mogens Steffensen

Received: 25 May 2022
Accepted: 10 August 2022
Published: 17 August 2022

1. Introduction

In 2021, the number of cyber attacks in Indonesia increased by 9.6% compared to 2020 (Honeynet 2022). The most common methods of cyberattack employ ransomware or data leaks. Cyberattacks can be directed at individuals, organizations, and countries (Yusgiantoro 2014), and can lead to financial losses, damaged reputations, or reduced service performance. Therefore, cybersecurity, which is the preservation of the confidentiality, integrity, and availability of information in cyberspace (ISO 27032:2012 2018), is critical for individuals, organizations, and countries.

The cyber environment is complex, and cyberattacks are increasing in both number and variety. There is therefore a need for cybersecurity awareness and a better understanding of cyber-vulnerabilities and threats to ensure the protection of information assets.

A key component of an information security management system (ISMS) is information security risk assessment (ISRA), which helps an organization identify key assets and quantifiably assess information security risks; this facilitates the development of risk management strategies (Shamala et al. 2015).

An ISRA may use a formal or a temporal approach. A formal approach focuses on the likelihood and severity of potential threats. On the other hand, the ISRA method's temporal approach employs direct testing to produce a risk value (Wangen et al. 2018). Formal risk assessments can be conducted in a number of ways, including a generic method that uses ISO 31010 and methods specifically designed for use in information security. Failure mode and effects analysis (FMEA); deplhi, hazard and operability study (HAZOP); fault tree analysis; and decision trees are a few examples of risk assessment techniques based on the

ISO 31010 guidelines (IEC/ISO 31010:2009 2009). The operationally critical threat, asset, and vulnerability evaluation (OCTAVE); factor analysis of information risk (FAIR); central computer and telecommunications agency (CCTA) risk analysis and management method (CRAMM), ISO 27005, and NIST 800-30 round methodologies are some other examples of ISRA techniques (Shameli-Sendi et al. 2016).

Several current studies use risk assessment methods with a formal approach, such as the common vulnerability score system with awareness of network security situations (Xi et al. 2018), incorporation of fault trees and fuzzy analysis for cyber security risks (de Gusmão et al. 2018), and the use of fuzzy FMEA for network security risk assessment (Silva et al. 2014). The results of the assessment and control of existing information security risks from formal techniques need to be tested regularly to evaluate whether the existing controls are still effective.

Temporal risk assessment techniques, which use direct testing, include audits, penetration testing, tabletop exercises, vulnerability assessments, and red teams (Wangen et al. 2018). In the latest study, the use of testing methods with a temporal approach is still separate. Several temporal methods exist, such as audit methods with fuzzy theory (Porcuna-Enguix et al. 2021), penetration testing methods for information security in an ecosystem (Knowles et al. 2016), and the use of tabletops for web-based learning (Borgardt et al. 2017).

The present study incorporates several direct testing techniques, including audits, tabletop exercises, and penetration testing, to present a framework for evaluating information security risks using a temporal approach. In this study, the ISMS is audited, the information security team's preparedness to respond to disasters is tested using tabletop exercises, and various components of information security technology are assessed using penetration testing; this research takes a case study of network security in several organizations in Indonesia. Tests using audit methods and penetration tests are carried out in government organizations, while tabletop exercise testing methods are carried out in private companies.

We developed a new framework based on Endley's situation awareness framework; this framework is used for risk assessment based on direct testing of existing controls with reference to the annex ISO 27001:2013.

The main contributions of this study are as follows:

1. Presenting a new framework for risk assessment based on cyber situational awareness in organizations
2. Developing an application that supports cybersecurity risk assessments.

This paper is structured as follows: The theoretical framework is presented in Section 2. Section 3 presents a risk assessment framework that can be used to improve a cybersecurity management system by incorporating a situational awareness model. Section 4 presents the results. Section 5 summarizes the conclusions and offers recommendations for future research.

2. Theoretical Framework

This theoretical framework is the basis for the development of this research. The first part discusses cyber situation awareness. The topic of cyber situation awareness provides the main basis for discussion of cyber security issues. The second section discusses risk assessment; this method is used to assess the results of the risk assessment of the condition of the network security environment. The third section discusses the ISO 27001:2013 information security management system. Within the framework of ISO 27001, there is an appendix that is used as a reference basis for controlling this research. The fourth section relates to the information system architecture used to implement the cybersecurity risk assessment.

2.1. Cyber Situational Awareness

Cybersecurity includes security for applications, the internet, and networks and is one aspect of information security (ISO 27032:2012 2018). Cybersecurity is a technology and

a process designed to protect assets such as computer hardware and software, networks, data, and online activities, all of which may be vulnerable to cybercrimes, terrorist groups, and hackers. Since the threats of attacks and cybersecurity vulnerabilities are uncertain, situational awareness is key to protecting information assets. Several studies on cybersecurity using situation awareness have been carried out in several fields such as network computing (Rapuzzi and Repetto 2018), cyber-physical systems (Kure et al. 2018), and management (Leszczyna 2018).

Situational awareness is perceiving environmental elements in terms of time and space, understanding their meaning, and projecting their status in the near future; it comprises three levels: perceiving elements in the environment, understanding the current situation, and projecting the future status to support decisions (Endsley 1995).

Situational awareness has technical and cognitive aspects; the technical aspects relate to collecting, compiling, processing, and combining data, while the cognitive aspect relates to a person's mental awareness and capacity in certain situations to understand the technical implications and draw conclusions to make the right decisions. CSA is the ability to recognize the current state of assets and cyberthreats (perception), the ability to understand the meaning of the situation and the impact of the threat (understanding), and the ability to project the future state of the threat or action (projection) (Jiang et al. 2022).

Another definition of CSA is that it is a type of situational awareness that focuses on the cyberworld. The cyberworld contains risks and uncertainties, so CSA is required (Franke and Brynielsson 2014). Figure 1 depicts Endsley's three-level model of situational awareness.

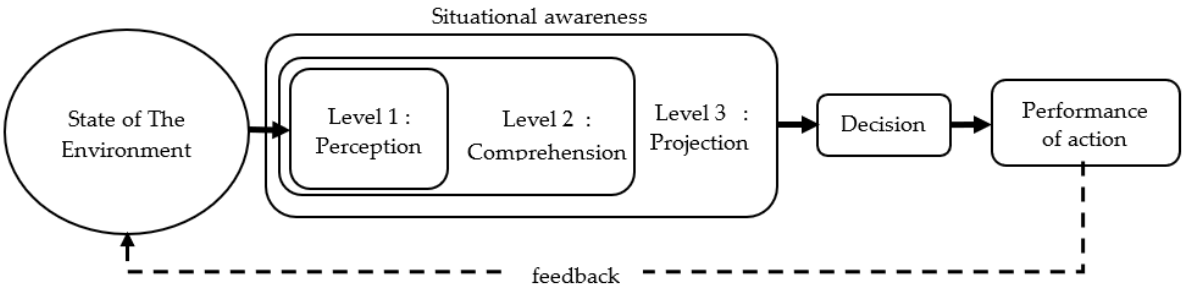

Figure 1. Three Levels of Situational Awareness (Jiang et al. 2022).

These three levels of situational awareness can be applied to the cyberworld as well:

1. Level 1: Perceiving the cyber environment; this perception involves identifying or detecting cyber environmental conditions.
2. Level 2: Understanding the meaning of the current situation. Perception reveals important information that helps users achieve their goals.
3. Level 3: Projecting the near future to support decisions. Information is extrapolated from an understanding of the cyber environment to determine the impact of the current status on future conditions.

CSA is complex because the cyberworld involves uncertainty, and users sometimes have inaccurate information (Figure 1). Since information about the cyberworld is imperfect, risk management is used to detect and prevent cyberattacks (Li et al. 2010).

Recent research, such as that by Webb et al., has developed the idea of information security risk management within the context of situational awareness by applying a situational awareness framework to information security in cyberspace (Webb et al. 2014). Burke et al. identify factors that must be taken into account in cyberspace to safeguard medical and patient data in order to improve situational awareness in the event of a cyberattack (Burke and Saxena 2021). An adaptive security framework is suggested by Griogoriadis et al. based on the circumstances of information security policy deployment; it comprises a risk assessment of the information security situation at sea (Griogoriadis et al. 2022). Chandra et al. use a situational awareness approach to help prioritize the risk of cyber-catastrophe and assess cyber-disaster simulations (Chandra et al. 2022).

This study also proposes a framework using CSA to develop network security risk assessment methods with temporal and application testing methods.

2.2. Risk Assessment

Risk is the effect of uncertainty on objectives. The effect is a positive, negative, or mixed deviation from what is expected. Risk management is a coordinated activity that directs and controls an organization's approach to handling risk (ISO 31000:2018 2018).

As illustrated in Figure 2, information security risk management comprises (i) establishing a context, (ii) assessing risk, which includes identifying, analyzing, and evaluating risk, (iii) treating risk, (iv) accepting risk, (v) communicating risk, and (vi) monitoring and reviewing risk (ISO 27005:2018 2018).

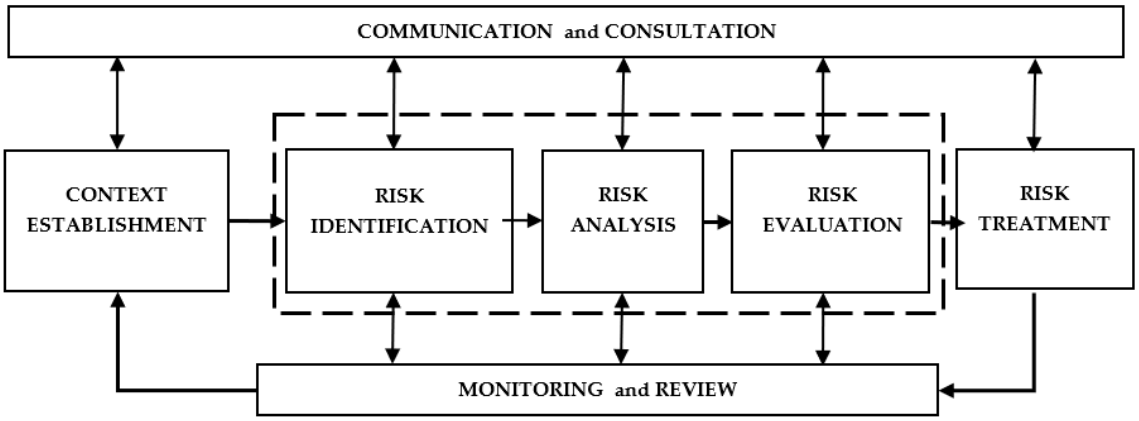

Figure 2. Risk Management Process of ISO 27005 (ISO 27005:2018 2018).

The context of information security risks in organizations has different objectives. Therefore, it is essential to consider the scope of implementing information security risk in an organization based on external and internal issues of the organization's environment and the stakeholders involved so that the implementation is more systematic, measurable, and controlled.

Risk assessment is an integral part of information security management, because it allows organizations to identify vulnerabilities and threats and analyze and control risks (Akinrolabu et al. 2019a). The risk assessment process based on ISO 27005 begins with risk identification, which entails identifying, accepting, and categorizing the risks and vulnerabilities that could prevent an organization from achieving its cybersecurity goals; these identified risks are then examined in a risk analysis.

Risk analysis is an attempt to understand the nature and behavior of risks, including the level of risk. The risk is analyzed based on two aspects: the impact on cybersecurity and the possibility of cybersecurity threats and vulnerabilities. Cybersecurity risk analysis may be qualitative, quantitative, or hybrid. Qualitative analysis is based on the experience and knowledge of risk owners; this approach results in less measurable data. Quantitative and hybrid analyses measure the value of impact, opportunity, and risk outcomes. A risk analysis generates a risk score based on the likelihood and potential consequences of cybersecurity threats and vulnerabilities (Computer Security Division 2012). A formal risk assessment considers a combination of likelihood and consequence.

After the risk analysis, risk is evaluated. In this stage, the results of the risk analysis will be compared with the predetermined risk criteria; this evaluation is used to choose to reduce the level of risk to an acceptable or tolerable level. Risk treatments may involve avoiding, sharing, modifying, and maintaining.

According to the ISO 27005 guidelines, communication and consultation involve an interactive process of information exchange used to understand the context of risk scope, risk assessment, and information security management; this process intends to

assist stakeholders in understanding risks and as an ingredient in making decisions to deal with risks.

Monitoring and review are also part of risk management; these steps ensure that the overall risk management process functions well and achieves the expected targets. Monitoring involves continuous observation of the cyber environment to identify possible cybersecurity threats and vulnerabilities. Monitoring can be continuous (i.e., the risk owner monitors the effectiveness of implemented controls or risk management tools) or separate (i.e., a third-party conducts monitoring in the form of testing).

There are two approaches to ISRA: high-level approaches and low-level approaches (Aksu et al. 2017). A high-level ISRA is a risk assessment based on a risk management process and provides general principles; this approach does not focus on quantitative risk measures or automation. In contrast, low-level ISRA places a greater emphasis on quantitative risk metrics and automation (Ramanauskaitė et al. 2021). Vulnerability management, which emphasizes quantitative security risk metrics, is one method of low-level risk assessment.

In addition to ISRA frameworks that use a high-level approach, several other risk assessment frameworks are found in the literature, such as risk assessment in cloud computing (Akinrolabu et al. 2019b), privacy data security (Jofre et al. 2021), information systems (Taherdoost 2021), and industrial control systems (Ji et al. 2022).

Several risk assessment methods use a low-level approach, such as open-source general vulnerability assessment systems (CVSS) (Walkowski et al. 2021), CVSS calculations using fuzzy logistic regression methods (Gencer and Başçiftçi 2021), and machine learning (Nikoloudakis et al. 2021).

This study uses a high-level ISRA based on information security controls ISO 27001:2013 and risk assessment ISO 27005. The ISO 27005 method was chosen because it is the most complete and widely used risk assessment approach (Wangen et al. 2018). The position of information security control risk assessment in the ISO 27005 information security risk management framework is shown in Figure 3.

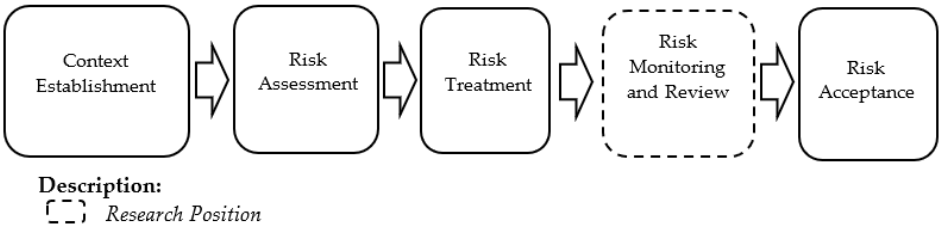

Figure 3. Research Position within the ISO 27005 Framework.

2.3. Information Security Management System ISO 27001:2013

The plan–do–check–action (PDCA) model is a general management model used in all ISO standards, including ISO 27001:2013 (Silva et al. 2020). The requirements of the ISO 27001:2013 ISMS, as based on the PDCA framework, are presented in Table 1.

Table 1 illustrates the components of the ISO 27001 and the corresponding phases of the PDCA model. The planning phase includes two elements: action to address risks and opportunities, and planning to achieve information security objectives. The implementation phase includes a number of components, including resources, expertise, awareness, communication, documented information, operational planning and control, ISRA, and information security risk management measures. The checking stage includes management review, monitoring, measurement, analysis, and assessment. Nonconformances and corrective actions, as well as continuous improvement, fall under the corrective action stage.

According to Table 1, the ISRA's position in the PDCA framework is in the implementation phase and in the risk treatment plan (clause 8.3). The ISRA used in this study refers to the annex ISO 27001:2013, which consists of 35 control objectives and 114 controls, as shown in Table 2 with a case study of network security.

Table 1. PDCA Framework and Element Requirements of ISO 27001 (ISO/IEC 27001:2013 2013).

Phase PDCA	Main	Clause	Element Requirements of ISO 27001
Plan	Plan	6.1	Actions to address risks and opportunities
		6.2	Information security objectives and planning to achieve them
Do	Support and Operation	7.1	Resources
		7.2	Competence
		7.3	Awareness
		7.4	Communication
		7.5	Documented information
		8.1	Operational planning and control
		8.2	Information security risk assessment
		8.3	Information security risk treatment
Check	Performance evaluation	9.1	Monitoring, measurement, analysis and evaluation
		9.2	Internal audit
		9.3	Management review
Action	Improvement	10.2	Nonconformity and corrective action
		10.3	Continual improvement

Table 2. Control of Annex ISO 27001:2013 (ISO/IEC 27001:2013 2013).

No.	Clauses	Control Objectives	Control
A.5	Information Security Policies	1	2
A.6	Organization of information security	2	7
A.7	Human resources security	3	6
A.8	Asset management	3	10
A.9	Access control	4	14
A.10	Cryptography	1	2
A.11	Physical and environmental security	2	15
A.12	Operations security	7	14
A.13	Communications security	2	7
A.14	System acquisition, development and maintenance	3	13
A.15	Supplier relationships	2	5
A.16	Information security incident management	1	7
A.17	Information security aspects of business continuity management	2	4
A.18	Compliance	2	8
	Total	35	114

2.4. Information Security Risk Control Testing

During the checking phase, it is determined whether or not an information security system is functioning properly. One way to do this is by auditing. The most common auditing technique in information security management is based on the ISO 19011:2018. The audit process includes several steps: (1) audit initiation, (2) audit preparation, (3) audit implementation and audit report, (4) completion of audit findings, and (5) follow-up (ISO 19011:2018 2018).

The initial stage of the audit includes coordination with the auditee and determining the feasibility of the audit. Audit preparation involves a written review that outlines the audit criteria, areas of concern, methods, the process or function to be audited, the risks and opportunities, the scope of the audit, and the audit objectives. During the preparation phase, the audit plan and audit objectives are defined; the media to be used in the audit are determined; it is decided whether the audit will be conducted on-site or remotely; and any

needed sampling standards are identified. Our goal is to assess the success of the control risk treatment strategy described in the ISO 27001:2013 Annex.

Audit implementation begins with the start of the audit and includes collecting and verifying information by reviewing documents, conducting field observations and interviews, developing an audit report, and closing the audit. The audit report informs the auditee of the audit results and define the length of time for corrections if nonconformities were identified. Audit results can be categorized as major findings, minor findings, or observations. A major finding is a high-risk factor; this includes unacceptable risks due to system breakdown. A minor value is a moderate risk value that is still acceptable but affects performance. Observations are audit findings that identify room for improvement; these have low risk values and are still acceptable. The audit is declared complete if the auditor and the auditee state that all activities, including audit findings to be corrected by the auditee, have been verified and declared acceptable by the auditor.

Exercise testing uses a simulation to test a team's preparedness to deal with cyber disasters. An exercise is an emergency simulation designed to validate the viability of an organization's information technology services. One type of exercise is a tabletop exercise. A tabletop exercise is a discussion-based simulation; personnel meet in a room to discuss their roles during an emergency and their responses to specific emergency situations (Grance et al. 2006). Cyber disaster simulation activities are sustainable organizational plans using information technology to serve customers securely. Organizational sustainability is an organization's ability to survive and remain competitive in the face of economic, social, environmental, ethical, and technological elements that can impact it both now and in the future (Corrales-Estrada et al. 2021). Sustainable organizations need simulations exercise to mitigate cyber disasters; this mitigation is used to support decisions so that disaster risk can be reduced (Caputo et al. 2018). The goal of current disaster simulation research is to improve people's or organizations' capacity for responding to emergencies (Poller et al. 2018; Musharraf et al. 2019; Afulani et al. 2020; Fogli et al. 2017; Skryabina et al. 2020; Gomes et al. 2014).

Our study used a tabletop exercise to measure organizations' readiness to deal with cyber disasters or attacks. A tabletop exercise is a discussion session amongst members of an organization who work together to address a particular issue. During the discussion, participants discussed their respective roles in increasing risk management awareness when dealing with cybersecurity incidents and certain emergencies. Several current studies using tabletop exercises in dealing with disaster incidents can use material aids (Sandström et al. 2014) and also web-based tools (Borgardt et al. 2017).

Penetration testing is an authorized simulation of an active cyberattack; it aims to assess cybersecurity and find hidden vulnerabilities (Zhou et al. 2021). There are several penetration testing methods, including black box, white box, and grey box. A black box is a penetration testing method in which the testing team is simply notified that there is a security breach. The testers are given only the name of the company but must obtain other information about the network and the target without assistance; this method is time-consuming and expensive. In white box penetration testing, the testing team is given all the information about the target to be tested and informed which infrastructure needs to be tested. In grey box penetration testing, the testing team is provided some information about the target being tested. In this study, the black box penetration test is used because the black box method is the closest to the real case.

Penetration testing involves numerous steps, including gathering information, assessing vulnerabilities, exploiting vulnerabilities, and analyzing the test. Figure 4 (Ghanem and Chen 2020) illustrates the steps of penetration testing.

During the information gathering stage, the testing team collects documents about the target; determines the scope, duration, and time of testing; chooses testing methods; and obtains documented approval for the test, nondisclosure agreements, and potential incidents. The testing team also collects the necessary information to analyze the target's vulnerabilities.

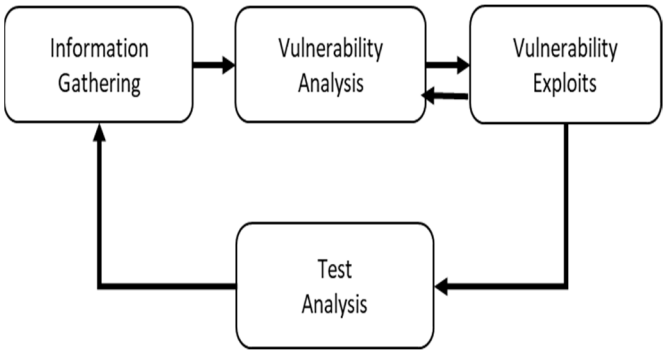

Figure 4. Penetration Testing Stages (Ghanem and Chen 2020).

In the vulnerability analysis stage, the testing team defines, identifies, and seeks to understand how vulnerabilities are created and discovered. The purpose of this analysis is to detect, eliminate, and avoid vulnerabilities. In the vulnerability analysis stage, a set of commands that take advantage of vulnerabilities and can cause harm to information assets are developed. Next, the results of the tests are analyzed to generate a vulnerability risk analysis and recommendations for corrective actions.

3. Materials and Methods

3.1. Risk Treatment Plan Testing Model with Cyber Situational Awareness Framework

This model was created to evaluate how well the predefined cybersecurity risks were protected against vulnerabilities. Controlling the risk treatment plan to lower the degree of risk to an acceptable level is how the risk assessment is carried out. To identify the control flaws in the existing risk treatment plan, periodic testing is necessary because to the quick changes in cyber conditions. Additionally, it makes the cybersecurity team more aware of the need to strengthen the control systems in the face of threats from cyberattacks and vulnerabilities; this adheres to the model of cyber situational awareness (Figure 5).

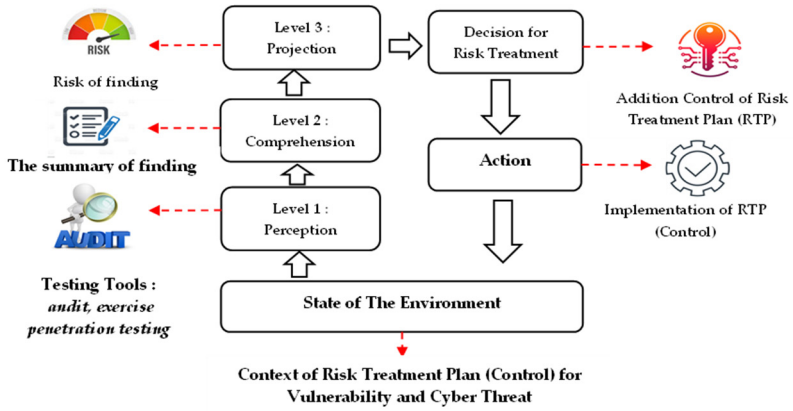

Figure 5. New Model of The Risk Treatment Plan Testing Framework with The Situational Awareness Model (Novelty).

According to the cyber situation awareness framework model, the first stage is to construct the control context for the risk management plan to be tested in order to ascertain the environmental circumstances. The second stage is perception, which includes testing techniques.

The third stage is the comprehension stage, where information concerning testing is gathered in order to learn more about the circumstances around the sample being examined. The fourth stage is projection, which involves performing a risk analysis to forecast cyber security performance; this evaluation is based on the findings from audits, exercises, and penetration tests regarding the vulnerabilities in the present risk treatment

plan control. The next step is the decision-making stage, where actions are planned and taken to strengthen the risk treatment plan's flaws and make it more robust in the face of the threat of cyberattacks.

The aforementioned model above can be made in the form of a relationship table between the Endsley model elements and the cyber situational awareness testing model (Table 3).

Table 3. Relationship Between the Elements of the Endsley Model and the Cyber Situational Awareness Testing Model.

Endsley Model	Cyber Situation Awareness Testing Model
State of Environment	Context of risk treatment plan
Perception	Testing Tools
Comprehension	Summary of testing findings
Projection	Risk Projection
Decision	Decision for risk treatment plan
Action	Correction Action

From Table 3, it is clear that the context of the risk assessment of this study is the risk assessment of network security controls. The testing methods used are audit, exercise, and penetration testing methods. Several tests will produce findings that will be summarized for risk value analysis. Figure 6 shows the relationship between testing and risk value.

Figure 6. Relationship Between the Risk Treatment Plan Testing Method and Risk Finding.

The risk assessment of the test findings needs to be determined by the criteria for the risk value that can be accepted or tolerated. The risk assessment criteria for this research can be shown in Table 4.

The level of risk from test findings is divided into three levels: low (weight: 100), medium (weight: 50), and high (weight: 0). In this study, a high level of risk is deemed unacceptable, whereas low and medium levels are considered acceptable.

From this risk category, we can calculate the total risk value of the risk treatment plan control based on Annex A ISO 27001:2013. The total risk value is an indicator of the extent to which the risk treatment plan control meets ISO 27001:2013 Annex A. The equation for the total risk value can be shown as follows:

$$Total\ Risk\ Value = \frac{\sum_{i=1}^{k} A_{accepted}}{\sum_{i=1}^{k} A_{total}} \quad (1)$$

where:

k = Sum of control from Annex

$A_{acceptable}$ = The total number of acceptable Annex A controls is the low (yellow) and medium (green)

A_{total} = The total number of controls from the Annex applied

The equation for the total risk value becomes the basis for the calculations used in the application.

Table 4. Criteria for the Level of Risk Resulting from Audit Findings, Exercises, and Penetration Tests.

Risk Level	Color Code	Weight	Risk Acceptance Level	Audit Criteria	Exercise Criteria	Penetration Testing Criteria
High (Red)		0	Unacceptable	System failure, affecting business termination or financial loss	Team awareness of cyber disasters does not exist such as knowledge, concern for reading the situation, mental condition, and support system	Impact on business termination or financial loss
Medium (Gree)		50	Acceptable	System inconsistencies or performance disruptions but no significant impact on the business	There is team awareness of cyber disasters but needs improvement	Performance disruptions but no significant impact on the business
Low (Yellow)		100	Acceptable	Opportunities for improvement or disruption but no impact on cybersecurity performance	Team awareness of cyber disasters is adequate and need to be maintained	Disruptions but no impact on cybersecurity performance

3.2. System Architecture Testing Risk Treatment Plan

In the design of our application, we built a system that combines several elements to accomplish a common goal. The risk assessment application developed in the present study runs on a web-based platform and codeIgniter version 4. The application made with codeIgniter was chosen because it was organized, open source, affordable, and came with the required libraries.

Figure 7 shows a flow chart of the risk assessment process, which includes asset valuation, risk identification, risk analysis, and risk control. Risk control is then tested. Effective corrective actions can reduce the risk to an acceptable level. A system architecture can be created from this flow diagram, as shown in Figure 8.

As shown in the data flow diagram in Figure 8, the user and the cybersecurity risks team are two actors who use the application. In addition to the level 0 data flow diagram, the level 1 data flow diagram is given in Figure 9 in order to provide a more thorough understanding of the system architecture.

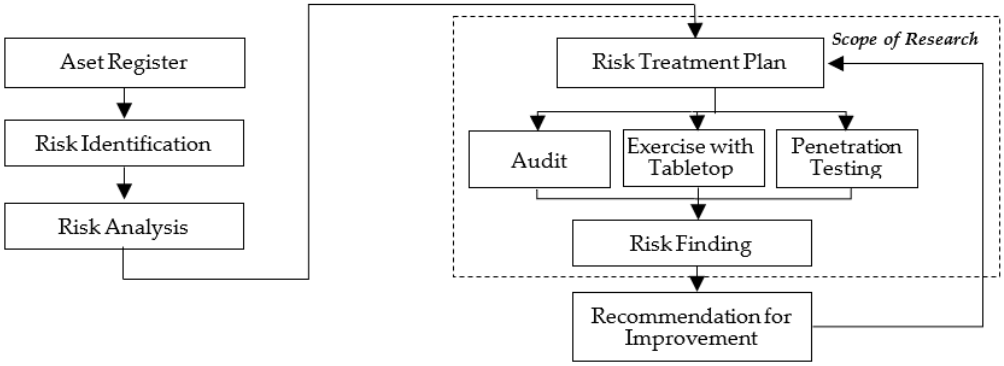

Figure 7. The Risk Management Flow Chart's Scope of the Risk Treatment Plan Testing Architecture System.

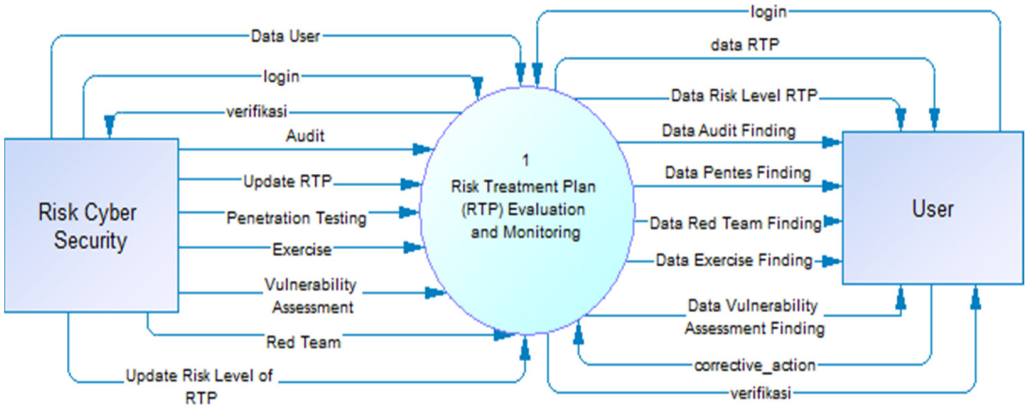

Figure 8. Data Flow Diagram Level 0.

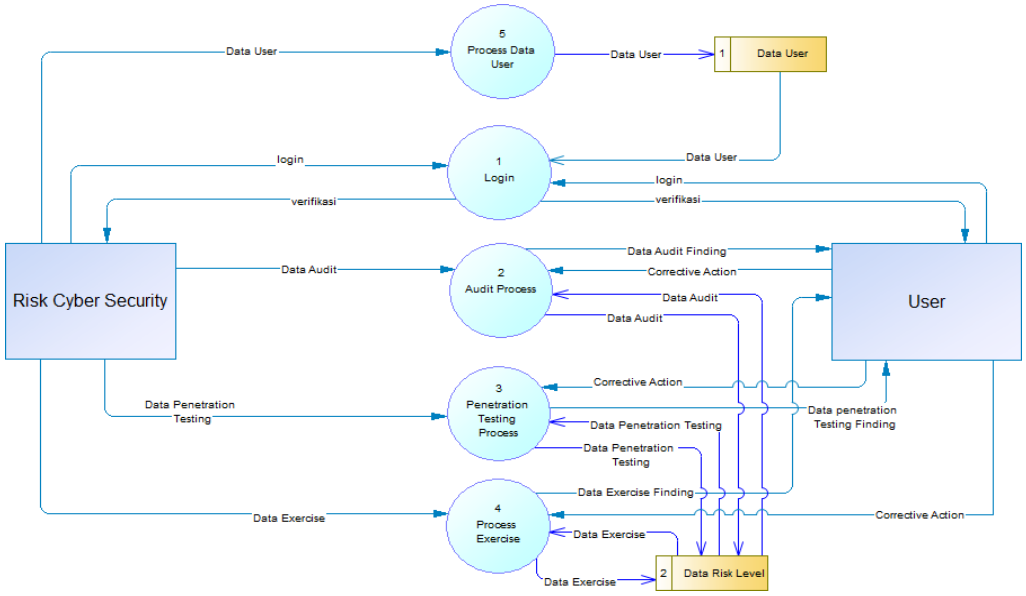

Figure 9. Data Flow Diagram of the Level 1 Testing Using Audit, Exercise and Penetration Testing.

The flow chart in Figure 9 illustrates how the cybersecurity risks enter and update the test findings in the application. The application generates a score and a risk rating based on the test results. Based on the updated results, the application then offers recommendations for corrective action to lower the risk level to either the lowest achievable level or an acceptable level.

Design an architectural system for testing the risk treatment plan, in addition to the data flow diagram above, a class diagram is also made to describe the contents of the database system in the application. The architecture of the application system class diagram of the risk treatment plan control test is shown in Figure 10.

3.3. Application Features Testing Risk Treatment Plan for Cyber Situational Awareness

To help assess risk, this study uses an application presented in Figure 11; this application presents menu of tests. In Annex ISO 27001:2013, there are control requirements from Annex A.5–A.18. The results of the risk treatment plan control test from Annex A.5. convey with A.18. will qualitatively produce the total index value and the level of risk. The categories of high, medium, and low-risk levels can be seen in the color of each annex. In the application, an attachment description of the findings and recommendations for improvement can also be shown so that the level of risk can be reduced to an acceptable level.

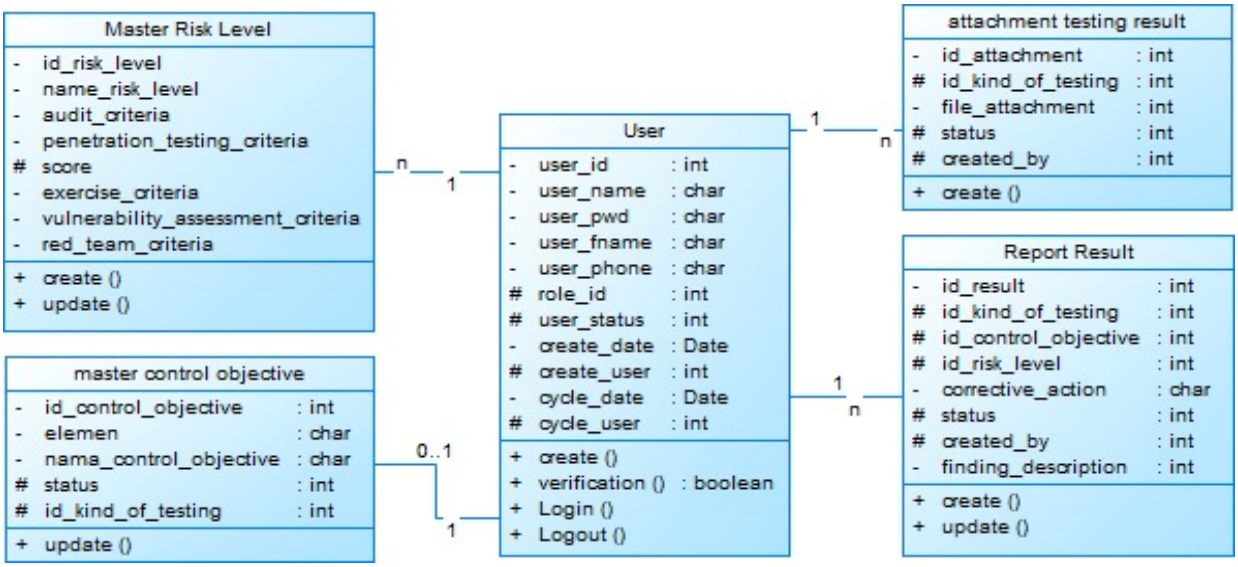

Figure 10. Class Diagram of Risk Treatment Plan Control Test Applications.

3.4. Network Security Case Study

Network security is part of a cybersecurity management system. In this study, the risk assessment of network security assets comprises information (I), people (P), hardware (H), software (S), tangible assets (T), and organizational reputation (R); this network security risk assessment was conducted in an organization in Indonesia. The results of the brainstorming by the information security team resulted in a table of risk identification and network security risk control (Appendix A, Table A1). On the basis of this table, a relationship table between control objectives that refer to Annex ISO 27001:2013 with audit testing, exercise, and penetration testing methods was made (Table A2).

Table A2 shows that Annex A controls A.5–A.18 that are relevant to the test are denoted by "v," while those that are not are denoted by "x". The audit method is referenced in Annexes A.5–A.18; this is denoted by "v". The exercise method is covered in Annexes A.6. and A.7., A.9, A.12, A.15, A.17. The penetration testing method is covered in Annexes A.9., A.10., and A.13.

After mapping the risk treatment plan control based on Annex ISO 27001:2013 with the testing method, the next stage is the implementation of network security control testing.

The first test was an audit based on Annex A.5–A.18 to verify that the controls are being implemented effectively. Referring to Annex ISO 27001:2013, the audit process was conducted by means of document review, observation, and interviews. The auditor has audit competence, such as lead auditor training and experience in auditing; this study provides an audit checklist based on Annex ISO 27001:2013. The results of the audit are in the form of an audit report.

The second test was the exercise test method with a tabletop. The topics taken in the tabletop exercise scenario were a ransomware and an earthquake disaster attack; this is based on brainstorming with the cyber disaster team. The stages of the scenario process are ransomware and earthquake threat testing scenarios, obtaining incident information, reporting problems, problem analysis, recovery, and activation process. The results reflect the extent of the team's preparedness in dealing with cyber disasters and findings for future improvements.

The third test was the penetration testing method; its purpose was to technically test information security systems against threats and identify potential failures in protecting assets. In this study, penetration testing was conducted using the black box method. The target of the attack is an IP address segment 10.10.25.0/24. The scope of the testing sampling is to check ports open or closed, check software version, operating system fingerprint, weak password, or authentication, and check vulnerability software. Each

vulnerability was exploited with step-by-step proof of concept, information gathering, and consequent impacts.

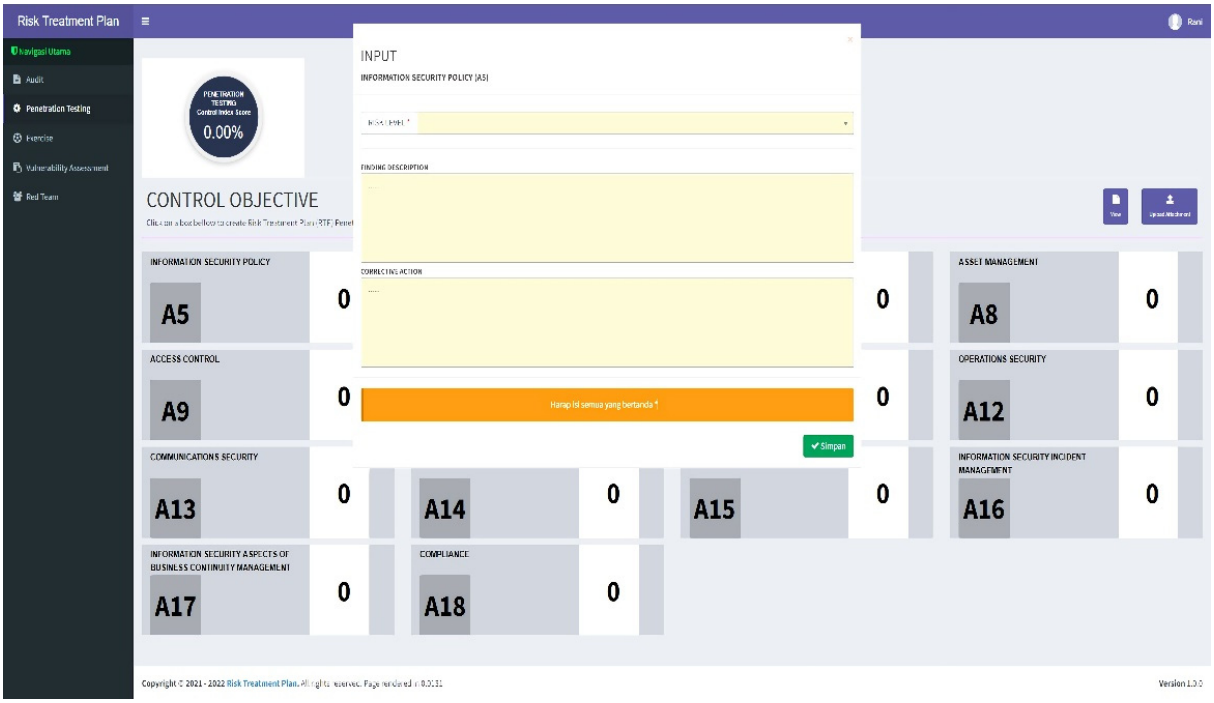

Figure 11. Application Features for Monitoring and Evaluating Risk Treatment Plan Controls.

4. Results

4.1. Risk Assessment Results

The risk levels for each test result are shown below based on the outcomes of testing the control of the risk treatment plan based on Annex ISO 27001:2013.

4.1.1. Results of the Audit Method

Cybersecurity testing in the case of network with the audit method result in the risk value of audit findings, as presented in Table 5.

Table 5. Risk Level of Audit Findings Control Risk Treatment Plan Network Security.

Element	Control Objectives	Risk Value	
		Score	Risk Level
A.5	Information security policies	0	High
A.6	Organization of information security	0	High
A.7	Human resources security	0	High
A.8	Asset management	0	High
A.9	Access control	50	Medium
A.10	Cryptography	50	Medium
A.11	Physical and environmental security	50	Medium
A.12	Operations security	50	Medium
A.13	Communications security	50	Medium
A.14	System acquisition, development, and maintenance	100	Low
A.15	Supplier relationships	50	Medium
A.16	Information security incident management	50	Medium
A.17	Information security aspects of business continuity management	50	Medium
A.18	Compliance	50	Medium

The results of the test using the audit method in Table 5 above are entered into the monitoring and evaluation application of the risk treatment plan visually, as shown in Figure 12.

Figure 12. Visual Monitoring of Risk Control Treatment Plan of Audit Results.

The results of the risk assessment using the audit method show that the security performance index score is 39.29% complies with the ISO 27001 annex's standards. The risk level is deemed high in Annex A controls A.5–A.8 and medium in A.9–A.18, except for A.14, where the risk was considered low (Table 5). After verifying the effectiveness of the results of the corrective action audit findings in controls with high and medium risk, the security performance index score fully complies with Annex ISO 2700:2013's standards.

4.1.2. Results of the Tabletop Exercise Method

As illustrated in Appendix B, cybersecurity testing using a tabletop approach yields a risk score (Table A3). The risk values from the table are then entered into the monitoring and evaluation application to control the risk management plan so as to produce a visual risk assessment (Figure 13).

The results of the risk assessment findings using the tabletop exercise method show that the security performance index score is 75% and complies with the ISO 27001 annex's standards. Several Annex A controls to ISO 27001:2013 related to exercise testing concluded that there was no high-risk value. The medium risk value is found in Annex organization of information security (A.6), human resources security (A.7) and information security aspects of business continuity management (A.17). For the Annex with low-risk values found in access control (A.9), operational Security (A.12) and supplier relationships (A.15). After verifying the effectiveness of the results of the corrective action exercise findings in controls with medium risk, the security performance index score fully complies with annex ISO 2700:2013's standards.

4.1.3. Results of the Penetration Testing Method

Cybersecurity testing using the penetration testing method resulted in the risk value of penetration testing findings as presented in Table 6.

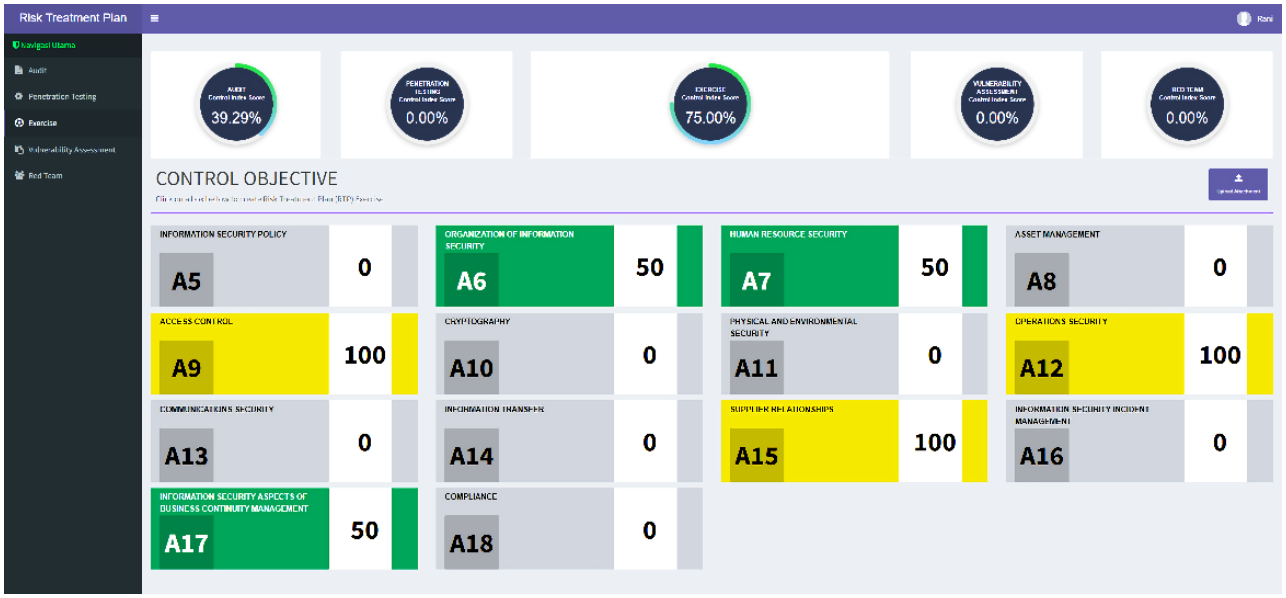

Figure 13. Visual Monitoring of Risk Control Treatment Plan of Tabletop Exercise Results.

Table 6. Risk Value of Network Security Penetration Testing Findings Based on Annex ISO 27001:2013.

No.	Findings	Annex A ISO 27001	Risk Level	Description
1	ScMM DSL Modem/Router Backdoor Detection	A.13. Communications security	High	Attackers can infiltrate the device and access sensitive data when the exploit is successfully executed
2	MS12-020: Remote desktop vulnerability that could allow executing code remotely	A.9. Access control	High	Attackers can infiltrate and access the target
3	Weak user dan password	A.9. Access control	High	Attacker can access web application with admin level
4	SNMP Agent Default Community Name (public)	A.13. Communications security	High	The attacker can obtain all the sensitive information contained in the target
5	Indikasi mining crypto currency	A.10. Cryptography	Medium	The device can run cryptocurrency mining automatically, draining hardware and CPU resources and internet connection

Based on Table 6, we enter the value of the risk findings into a monitoring and evaluation application for the control of the risk treatment plan to produce a visual risk assessment (Figure 14).

Figure 14 shows that the results of testing with penetration testing show that the security performance index score is 16.66% complies with the ISO 27001 annex's standards. The results reveal a high risk in Annex A controls A.9 and A.13 and medium risk in A.10. After verifying the effectiveness of the results of the corrective action penetration testing findings in controls with medium risk, the security performance index score fully complies with annex ISO 2700:2013's standards.

4.1.4. Results of Testing Improvements with Audit, Exercise and Penetration Testing

The results of the improvement in the findings of network security control testing after correctives action have resulted in a reduction in the level of risk, as shown in Table 7.

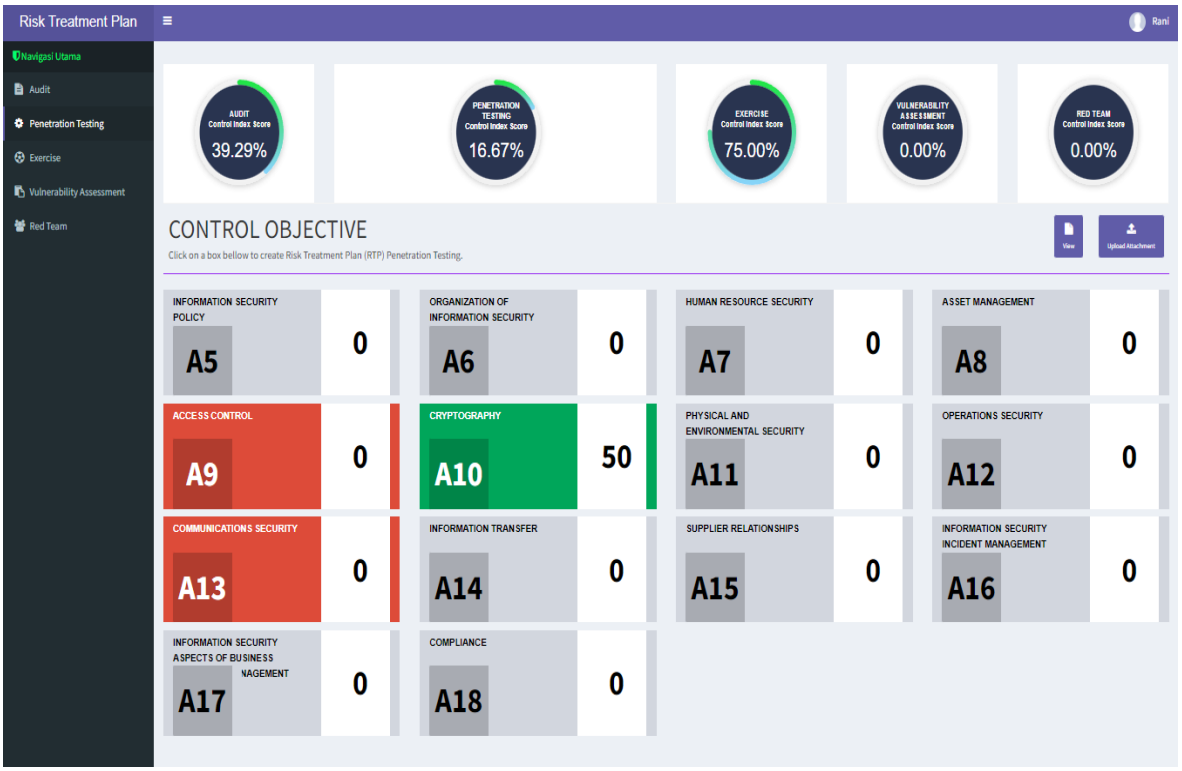

Figure 14. Visual Monitoring of Risk Control Treatment Plan of Penetration Testing Results.

4.2. Model Development Results

The cybersecurity control risk assessment process uses a temporal approach with audit, exercise, and penetration testing methods. The audit method is used to test the cybersecurity management system, the exercise method is used to test the level of team preparedness when facing a disaster, and the penetration testing method is used to test the control of technical aspects.

The results of a risk assessment are assisted by a risk assessment application to help monitor the risk value and the improvements made so that the risk value can be reduced to an acceptable risk level and improve cybersecurity performance. The results of this assessment show that a temporal risk assessment can be conducted through tests. The risk assessment of several test methods can help analyze the understanding comprehensively so that it can be used to predict cybersecurity conditions for the risk of cyber vulnerabilities and threats of cyberattacks. The results of this assessment included corrective actions to improve cybersecurity controls; this process produces a risk assessment framework that refers to the cyber situational awareness stage.

Table 7. An example of the findings and verifications from an improved network security test.

No	Non-Conformance of Testing Findings	Testing Type	Initial Scores	Initial Risk Level	Annex of ISO 27001:2013	Corrective Action	Personal in Charge	Status of Corrective Action	Residual Scores	Residual Risk Level
1	Information security policy has not been established	Audit	0	High	A.5. Information security policies	Establish an Information Security Policy, socialized, reviewed regularly regarding the effectiveness of the policy and documented.	Networks Security	Information security policy has been established	100	Low
2	Employee recruitment is carried out using an existing mechanism following regulations, namely ISO 27001:2013 requiring a screening/background checking process to ensure potential criminal acts; however, there has been no statement regarding organizational confidentiality that has been included in the statement and is connected to company regulations regarding indiscipline actions following information security rules. Information security competency standards have not yet been established	Audit	0	High	A.7. Human resource security	Make a statement letter to maintain the confidentiality of information assets and competency standards related to information security	Human Resources	A letter of agreement has been set for maintaining confidentiality and setting competency standards	100	Low
3	Some users don't fully understand attack ransomware	Tabletop Exercise	50	Medium	A.7. Human resource security	Raising user awareness through ransomware threat training and campaigns	Human Resources	Training and campaigns have been conducted and the team more understanding of ransomware and how to prevention	100	Low
4	The mechanism for teleworking regulations is not yet clear	Tabletop Exercise	50	Medium	A.6. Organization of information security	Improvement of teleworking rule policy	Networks Security	Rule and Policies for teleworking have been established and socialization	100	Low
5	ScMM DSL Modem/Router Backdoor. Detection.Attackers can infiltrate the device and access sensitive data when the exploit is successfully executed	Penetration Testing	0	High	A.13. Communication security	Related devices need to be updated	Networks Security	Vendor device-related have been conducted updated	100	Low
6	Weak user dan password. The user credentials used are still too weak and general	Penetration Testing	0	High	A.9. Access control	passwords can't be easy predictable and too general. password using standard password complexity so that it is not easy to guess	Networks Security	Passwords have been changed with rules that are not easy to guess. Recommendations for more than 6 numbers and combinations of numbers, symbols, uppercase, and lowercase lette	100	Low

From the example Table 7. The above shows that the recommendation for corrective action after verification of the final risk value is low, meaning that the risk level is acceptable.

5. Conclusions and Future Research

5.1. Conclusions

This paper presents a new framework for assessing control risk from a risk treatment plan; this framework model refers to Endsley's situational awareness model, which comprises perception, comprehension, projection, decision, and performance action. The first stage of this study is the perception process using direct testing. The scope of the testing of this study is the condition of controlling the risk treatment plan on the network security of an organization. The next stage is to analyze the findings of the three methods to determine the risk level of each control being tested. The results are then entered into the application for monitoring and evaluating risk management controls based on Annex ISO 27001:2013. The application will display a dashboard of which controls have acceptable and unacceptable risks and the index value of the control resilience condition from the risk treatment plan.

For any control with unacceptable risk, namely a high level of risk, recommendations for improvement are made to lower the risk level to acceptable—i.e., medium- or low-risk.

The network security case study shows that the audit risk level has a security performance index score of 38.46%, which complies with the ISO 27001 annex's standards; this performance index shows that several control values are categorized as an unacceptable risk. The unacceptable risk controls with high risk are information security policy (A.5), organization of information security (A.6), human resource security (A.7) and asset management (A.8). Meanwhile the medium risk value is annex access control (A.9), cryptography (A.10), environmental and physical safeguards (A.11), operational security (A.12), communication security (A.13), relations with suppliers (A.15), information security incident management (A.16), business continuity management from information security aspect (A.17), compliance (A.18); moreover, the low-risk value occurs in annex system acquisition, development and maintenance (A.14).

Testing the exercise method with tabletops indicates that the level of the security performance index score is 75% complies with the ISO 27001 annex's standards; this performance index shows that several control values are categorized as a medium-risk but there is no high-risk value. The medium risk value is found in annex information security organization (A.6), information security resources (A.7) and business continuity management from the information security aspect (A.17). For the annex with low-risk values found in access control (A.9), operational security (A.12) and relationship with suppliers (A.15).

The the penetration testing method demonstrate that the risk level of the security performance index score is 16.66% complies with the ISO 27001 annex's standards; this performance index shows that several control values are categorized as an unacceptable risk. The unacceptable risk controls with high risk are access control (A.9) and communications security (A.13). Meanwhile, the medium risk value is found in annex cryptography (A.10) and there is no low-risk value.

After verification of the effectiveness of corrective actions or recommendations for improvement of audit findings, exercises, and penetration testing with high and medium value categories, the security performance index has met 100% of ISO 27001:2013 annexes. The application has increased cyber situational awareness in monitoring and evaluating the effectiveness of implementing the risk treatment plan for network security assets.

The situational awareness framework has proven to describe the process from testing network security controls to generating the risk value of the test results. The risk assessment of the results of the test is an indicator of network security vulnerabilities.

The main contribution of this study is the availability of a new framework concept for conducting cybersecurity risk assessments based on cyber situational awareness and assisted by an application.

The direct testing improves the detection of vulnerabilities in cybersecurity control conditions from the system management, team preparation, and technical aspects. The risk

assessment using the testing method and the situation awareness framework of this study helps improve a more comprehensive risk assessment analysis, which is complementary to the formal risk assessment approach.

5.2. Future Research

Future developments in research include the following:

1. The scope of this study is the risk management process, a high-level strategy. In the future, it will be important to combine the common vulnerability score system method with low-level approaches like risk metrics.
2. Develop a risk assessment for the country's physical security using both a high-level and low-level risk assessment strategy.
3. Added additional test techniques, such as vulnerability analysis
4. Comparing audit, penetration testing, vulnerability assessment, and exercise outcomes to incident risk and risk test results.

Author Contributions: Conceptualization, N.A.C. and K.R.; methodology, N.A.C.; Software, N.A.C.; validation, A.A.P.R., T.S.G. and K.R.; supervision, A.A.P.R. and K.R.; writing—original draft, N.A.C.; writing—review & editing, A.A.P.R., T.S.G. and K.R.; funding acquisition, A.A.P.R. and K.R. All authors have read and agreed to the published version of the manuscript.

Funding: The University of Indonesia under the International Indexed Publications (PUTI) grand Q2 2022 (reference NKB-677/UN2.RST/HKP.05.00/2022).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This paper is fully supported and funded by the University of Indonesia under the International Indexed Publications (PUTI) grand Q2 2022 (reference NKB-677/UN2.RST/HKP.05.00/2022). All Individuals have consented to the acknowledgement.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Risk Identification and Risk Control for Network Security.

Asset Number	Asset Name	Threat	Vulnerability	Risk Potential	Risk Treatment	Annex ISO 27001
I1	Network Documentation	Data Lost	No Update	A: Document not available	Backup, provide information classification procedure	A.6. Organization Information Security A.8. Asset management A.12. Operations security
I2	Availability Report	Data Lost	No Update	A: Document not available	Backup, provide information classification procedure	A.8. Asset management A.12. Operations security
I3	E Ticketing	System Down, Data Lost/Breach	No system Ticketing	C: Data breach A: Service not available	Backup and Capacility Planning	A.8. Asset management A.12. Operations security
P1	IT Manager	Social Engineering	NDA	C: Data leak	Awarness and NDA	A.7. Human resource security
P2	Help desk	Social Engineering	NDA	C: Data leak	Awarness and NDA	A.7. Human resource security A.12. Operations security A.16. Information security incident management
P3	Security Network	Sabotage	NDA	C: Network traffic data leaked from outside, sabotage from internal I: Data can be changed trough network probe A: System compromised and not available	Awarness and NDA	A.7. Human resource security A.11. Physical and environmental security A.12. Operations security A.13. Communications security A.16. Information security incident management
H1	Server 1	Psychical Threat, Sabotage	No server room	A: service not available	Provide Secure Areas for server, Hardware Maintaining	A.11. Physical and environmental security A.13. Communications security A.15. Supplier Relationship

Table A1. *Cont.*

Asset Number	Asset Name	Threat	Vulnerability	Risk Potential	Risk Treatment	Annex ISO 27001
H2	Server 2	Compromised, Sabotaged	No log report	C: Server Sabotage I: Data can be changed by unauthorized parties A: Data losses	Provide log activity, log server, password, log Monitoring	A.11. Physical and environmental security A.13. Communications security A.15. Supplier Relationship
H3	Security Aplliances Firewall	Compromised	No Install Firewall	C: Compromised Network and network Traffic I: No Firewall can cause malicious packet going in trough network traffic A: Service availability is threatened	Install and Configure Firewall Feature, Configure Firewall rules	A.10. Cryptography A. 13. Communications security
H4	Network Appliance Router	Compromised	No password	C: Confidentiality data are threatened A: Compromised router can cause Network Services Down	Give strong password for router admin login	A.11. Physical and environmental security A.13. Communications security
H5	Network Appliance Switch	Compromised	Sabotase	A: Service availability is threatened	Physical protectionto Switch device	A.11. Physical and environmental security A.13. Communications security
H6	Network Appliance Access Point	Compromised	Sabotase	A: Service availability is threatened	Physical protectionto the device, and give strong password for admin login	A.11. Physical and environmental security A.13. Communications security
H7	UPS1	Broken Device	Not Available	A: Service availability is threatened	Hardware Maintaining and Renewal	A.11. Physical and environmental security A.13. Communications security
H8	Computer1 Destop	Compromised and Sabotaged	No Password	C: accessed by unauthorized people I: Incomplete Data A: Data not available	Enable password and lock screen features, Clear desk and Screen Procedure	A.9. Access control A.11. Physical and environmental security
S1	Software for Wifi	Compromised	No Update	A: Service availability is threatened	Update Software Patch	A.13. Communications security
T1	Network	third party fraud	NDA	C: Data Leak A: Services Not Available	Provide NDA Vendor, Procedure Third Party/Outsourcing Vendor	A.15. Supplier relationships

Table A1. *Cont.*

Asset Number	Asset Name	Threat	Vulnerability	Risk Potential	Risk Treatment	Annex ISO 27001
R1	Reputation	Data Breach, Business Continuity	No Public Communication	C: Data Accidentally Leaked by Internal Employee	Communicate with client and public Provide Customer Service Provide Awarness for employee Provide Communications security Procedure	A.7. Human resource security A.13. Communications security A.17. Information Security aspects of business continuity A.18. Compliance

Table A2. Mapping the Relationship between Risk Treatment Plan Control with Testing Method.

No.	Control Objectives	Risk Treatment Plan for Network Security	Testing Result (V Related), (X Not Related)		
			Audit	Exercise	Penetration Testing
A.5	Information security policies	A set of policies for information security, published, communicated, and review	V	X	X
A.6	Organization of information security	Jobdesciption, Stakeholder contact, Rule, Policy to Teleworking, and mobile device	V	V	X
A.7	Human resources security	NDA, Background Checking, Disipline, Exit Clearance	V	V	X
A.8	Asset management	Asset Register, classification information, media handling	V	X	X
A.9	Access control	User Access Policy	V	V	V
A.10	Cryptography	Crypthography policy and key management	V	X	V
A.11	Physical and environmental security	Security Area, Removal Asset, Cabling Security, Clear and Desk Policy	V	X	X
A.12	Operations security	Operating Procedure, protection from Malware, Back Up, Log Monitoring, Control of sofware for networks, technicals vulnerabiliy, and audit	V	V	X
A.13	Communications security	Networks Security and Information Transfer	V	X	V
A.14	System acquisition, development, and maintenance	Application related with security, Securing application services on public networks, Test of data	V	X	X
A.15	Supplier relationships	NDA, Supplier Relationship and Delivery	V	V	X
A.16	Information security incident management	Incident and Improvement	V	X	X
A.17	Information security aspects of business continuity management	Business Continuity Plan and Redunance	V	V	X
A.18	Compliance	Compliance Legal and Review	V	X	X

Appendix B

Table A3. Risk Value of Network Security Tabletop Exercise Findings Based on Annex ISO 27001:2013.

No.	Tabletop Exercise Results	Disaster Type	Team	Endsley's Situational Awareness Factor	Annex ISO 27001:2013	Risk Value	Risk Level	Recomendation
1	Some users do not fully understand about ransomware	ransomware	user	situational awareness	A.7. Human resources security	50	medium	Raising user awareness through ransomware threat training and campaigns
2	• Ransomware situations are situations that have not been stated in the Disaster Recovery Plan document	ransomware	disaster recovery team	system	A.17. Information security aspects of business continuity management	50	medium	Improved disaster recovery plan documents covering ransomware threat situations resulting in service outages, cybercrime, recovery processes, and equipment used for shutdown and disaster recovery
	• The priority process for recovering ransomware and earthquake cyber disasters is described in the Disaster Recovery Plan document	ransomware and earthquakes				50	medium	
	• There are no specific tool instructions for shutting down and recovering in the event of ransomware	ransomware				50	medium	
3	Requires training on rules and responsibilities related to recovery of ransomware threats that result in service outages and cybercrime	ransomware	human resources	knowledge	A.6. Organization of information security	50	medium	Training and improvement of duties and responsibilities related to handling the threat of ransomware attacks

Table A3. *Cont.*

No.	Tabletop Exercise Results	Disaster Type	Team	Endsley's Situational Awareness Factor	Annex ISO 27001:2013	Risk Value	Risk Level	Recomendation
4	The vendors involved already have a nondisclosure agreement (NDA)	ransomware	procurement	system	A.15. Supplier relationships	100	low	NDA expiration monitoring
5	Back up data has been performed regularly	ransomware	operational	system	A.12. Operations security	100	low	maintain
6	The mechanism for teleworking regulations is not yet clear	ransomware	operational	system	A.6. Organization of information security	50	medium	Need improvement of teleworking rules policy
7	Assignment of user access privileges has been set and is running well	ransomware	operational	system	A.9. Access control	100	low	maintain
8	Data center vendor control, servers have been evaluated regularly and are running well	ransomware and earthquakes	operational	system	A.12. Operations security	100	low	maintain
9	Information coordination mechanisms between OSH and IT recovery need to be established	earthquakes	operational	system	A.6. Organization of information security	50	medium	Improvement of Disaster Recovery Plan document covering earthquake threat situation
10	Provision of a crisis place in the event of an earthquake that results in an incapable building needs to be evaluated by a safer location from the earthquake	earthquakes	operational	system	A.17. Information security aspects of business continuity management	50	medium	Improvements for evaluating the location of the crisis center in the event of an earthquake

References

Afulani, Patience A., Jessica Dyer, Kimberly Calkins, Raymond A. Aborigo, Brienne Mcnally, and Susanna R. Cohen. 2020. Provider knowledge and perceptions following an integrated simulation training on emergency obstetric and neonatal care and respectful maternity care: A mixed-methods study in Ghana. *Midwifery* 85: 102667. [CrossRef]

Akinrolabu, Olusola, Jason R. C. Nurse, Andrew Martin, and Steve New. 2019a. Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security* 87: 101600.

Akinrolabu, Olusola, Steve New, and Andrew Martin. 2019b. CSCCRA: A Novel Quantitative Risk Assessment Model for SaaS Cloud Service Providers. *Computers* 8: 66. [CrossRef]

Aksu, M. Ugur, M. Hadi Dilek, E. İslam Tatlı, Kemal Bicakci, H. Ibrahim Dirik, M. Umut Demirezen, and Tayfun Aykır. 2017. A Quantitative CVSS-Based Cyber Security Risk Assessment Methodology For IT Systems. Paper presented at the 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, October 23–26.

Borgardt, James, Jodi Canaday, and David Chamberlain. 2017. Results from the second Galaxy Serpent web-based table top exercise utilizing the concept of nuclear forensics libraries. *Journal of Radioanalytical and Nuclear Chemistry* 311: 1517–24. [CrossRef]

Burke, George, and Neetesh Saxena. 2021. Cyber Risks Prediction and Analysis in Medical Emergency Equipment for Situational Awareness. *Sensor* 21: 5325. [CrossRef]

Caputo, Francesco, Luca Carrubbo, and Debora Sarno. 2018. The influence of cognitive dimensions on the consumer-SME relationship: A sustainability oriented view. *Sustainability* 10: 3238. [CrossRef]

Chandra, Nungky Awang, Anak Agung Putri Ratna, and Kalamullah Ramli. 2022. Development and Simulation of Cyberdisaster Situation. *Sustainability* 14: 1133. [CrossRef]

Computer Security Division. 2012. *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology Special Publication 800-30 Revision 1. Washington, DC: Computer Security Division, p. I-1.

Corrales-Estrada, Ana Maria, Loyda Lily Gómez-Santos, Cesar Augusto Bernal-Torres, and Jaime Eric Rodriguez-López. 2021. Sustainability and resilience organizational capabilities to enhance business continuity management: A literature review. *Sustainability* 13: 8196. [CrossRef]

de Gusmão, Ana Paula Henriques, Maisa Mendonça Silva, Thiago Poleto, Lúcio Camara e Silva, and Ana Paula Cabral Seixas Costa. 2018. Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management* 43: 248–60. [CrossRef]

Endsley, Mica R. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors Journal* 37: 32–64. [CrossRef]

Fogli, Daniela, Claudio Greppi, and Giovanni Guida. 2017. Design patterns for emergency management: An exercise in reflective practice. *Information & Management* 54: 971–86.

Franke, Ulrik, and Joel Brynielsson. 2014. Cyber situational awareness e A systematic review of the literature. *Computer & Security* 46: 18–31.

Gencer, Kerem, and Fatih Başçiftçi. 2021. The fuzzy common vulnerability scoring system (F-CVSS) based on a least squares approach with fuzzy logistic regression. *Egyptian Informatics Journal* 22: 145–53. [CrossRef]

Ghanem, Mohamed C., and Thomas M. Chen. 2020. Reinforcement Learning for Efficient Network Penetration Testing. *Information* 11: 6. [CrossRef]

Gomes, José Orlando, Marcos Borges, Gilbert J. Huber, and Paulo Victor R. Carvalho. 2014. Analysis of the resilience of team performance during a nuclear emergency response exercise. *Applied Ergonomics* 45: 780–88. [CrossRef]

Grance, Timothy, Tamara Nolan, Kristin Burke, Rich Dudley, Gregory White, and Travis Good. 2006. *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, Special Publication (NIST SP)*; Gaithersburg: National Institute of Standards and Technology. Available online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50889 (accessed on 16 March 2021).

Griogoriadis, Christos, Romain Laborde, Antonin Verder, and Panayiotis Kotzanikolaou. 2022. An Adaptive, Situation-Based Risk Assessment and Security Enforcement Framework for the Maritime Sector. *Sensor* 22: 238. [CrossRef]

Honeynet. 2022. Available online: https://honeynet.bssn.go.id (accessed on 12 January 2022).

IEC/ISO 31010:2009. 2009, *Guidelines for Risk Management—Risk Assessment Techniques*. Geneva: ISO, p. 22.

ISO 19011:2018. 2018, *Guidelines for Auditing Management Systems*. Geneva: ISO, p. 8.

ISO 27005:2018. 2018, *Information Technology—Security Techniques—Information Security Risk Management by International Electrotechnical Commission*. Geneva: ISO, p. 1.

ISO 27032:2012. 2018, *Guidelines for Cybersecurity*. Geneva: ISO, pp. 5–11.

ISO 31000:2018. 2018, *Risk Management-Guideline by International Electrotechnical Commission*. Geneva: ISO, p. 1.

ISO/IEC 27001:2013. 2013, *Information Technology—Security Techniques—Information Security Management Systems—Requirements*. Geneva: ISO, p. iii.

Ji, Xudong, Hongxing Wei, Youdong Chen, Xiao-Fang Ji, and Guo Wu. 2022. Three-Stage Dynamic Assessment Framework for Industrial Control System Security Based on a Method of W-HMM. *Sensor* 22: 2593. [CrossRef]

Jiang, Liuyue, Asangi Jayatilaka, Mehwish Nasim, Marthie Grobler, Mansooreh Zahedi, and M. Ali Babar. 2022. Systematic Literature Review on Cyber Situational Awareness Visualizations. *IEEE Access* 10: 57525–54. [CrossRef]

Jofre, Marc, Diana Navarro-Llobet, Ramon Agulló, Jordi Puig, Gustavo Gonzalez-Granadillo, Juan Mora Zamorano, and Ramon Romeu. 2021. Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach. *Applied Sciences* 11: 6699. [CrossRef]

Knowles, William, Alistair Baron, and Tim McGarr. 2016. The simulated security assessment ecosystem: Does penetration testing need standardisation? *Computers & Security* 62: 296–316.
Kure, Halima Ibrahim, Shareeful Islam, and Mohammad Abdur Razzaque. 2018. An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Science* 8: 898. [CrossRef]
Leszczyna, Rafał. 2018. Standards on cyber security assessment of smart grid. *International Journal of Critical Infrastructure Protection* 22: 70–89. [CrossRef]
Li, Jason, Xinming Ou, and Raj Rajagopalan. 2010. Uncertainty and Risk Management in Cyber Situational Awareness. In *Cyber Situational Awareness*. New York: Springer, pp. 51–68.
Musharraf, Mashrura, F. Khan, and Brian Veitch. 2019. Modeling and simulation of offshore personnel during emergency situations. *Safety Science* 111: 144–53. [CrossRef]
Nikoloudakis, Yannis, Ioannis Kefaloukos, Stylianos Klados, Spyros Panagiotakis, Evangelos Pallis, Charalabos Skianis, and Evangelos K. Markakis. 2021. Towards a Machine Learning Based Situational Awareness Framework for Cybersecurity: An SDN Implementation. *Sensor* 21: 4939. [CrossRef]
Poller, B., S. Hall, C. Bailey, S. Gregory, Richard Clark, P. Roberts, A. Tunbridge, V. Poran, B. Crook, and C. Evans. 2018. 'VIOLET': A fluorescence-based simulation exercise for training healthcare workers in the use of personal protective equipment. *Journal of Hospital Infection* 99: 229–35. [CrossRef]
Porcuna-Enguix, Luis, Elisabeth Bustos-Contell, José Serrano-Madrid, and Gregorio Labatut-Serer. 2021. Constructing the Audit Risk Assessment by the Audit TeamLeader When Planning: Using Fuzzy Theory. *Mathematics* 9: 3065. [CrossRef]
Ramanauskaitė, Simona, Neringa Urbonaitė, Šarūnas Grigaliūnas, Saulius Preidys, Vaidotas Trinkūnas, and Algimantas Venčkauskas. 2021. Educational Organization's Security Level Estimation Model. *Applied Science* 11: 8061. [CrossRef]
Rapuzzi, Riccardo, and Matteo Repetto. 2018. Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. *Future Generation Computer Systems* 85: 235–49. [CrossRef]
Sandström, Björn E., Håkan Eriksson, Lena Norlander, Mirko Thorstensson, and Gudrun Cassel. 2014. Training of public health personnel in handling CBRN emergencies: A table-top exercise card concept. *Environment International* 72: 164–69. [CrossRef]
Shameli-Sendi, Alireza, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. 2016. Taxonomy of information security risk assessment (ISRA). *Computer & Security* 57: 14–30.
Shamala, Palaniappan, Rabiah Ahmad, Ali Hussein Zolait, and Shahrin bin Sahib. 2015. Collective information structure model for Information Security Risk Assessment (ISRA). *Journal of Systems and Information Technology* 17: 193–219. [CrossRef]
Silva, Maisa Mendonça, de Gusmão, Ana Paula Henriquesde Gusmão, Thiago Poleto, Lúcio Camara e Silva, and Ana Paula Cabral SeixasCosta. 2014. A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management* 34: 733–40. [CrossRef]
Silva, Cláudia, José Magano, Anna Moskalenko, Teresa Nogueira, Maria Alzira Pimenta Dinis, and Hélder Fernando Pedrosa e Sousa. 2020. Sustainable Management Systems Standards (SMSS): Structures, Roles, and Practices in Corporate Sustainability. *Sustainability* 12: 5892. [CrossRef]
Skryabina, Elena A., Naomi Betts, Gabriel Reedy, Paul Riley, and Richard Amlôt. 2020. The role of emergency preparedness exercises in the response to a mass casualty terrorist incident: A mixed methods study. *International Journal of Disaster Risk Reduction* 46: 101503. [CrossRef] [PubMed]
Taherdoost, Hamed. 2021. A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection. *Electronic* 10: 3065. [CrossRef]
Walkowski, Michał, Jacek Oko, and Sławomir Sujecki. 2021. Vulnerability Management Models Using a Common Vulnerability Scoring System. *Applied Science* 22: 8735. [CrossRef]
Wangen, Gaute, Christoffer Hallstensen, and Einar Snekkenes. 2018. A framework for estimating information security risk assessment method completeness, Core Unified Risk Framework, CURF. *International Journal Information Security* 17: 681–99. [CrossRef]
Webb, Jeb, Atif Ahmad, Sean B. Maynard, and Graeme Shanks. 2014. A Situation awareness model for information security risk management. *Computers & Security* 44: 1–15.
Xi, Rongrong, Xiaochun Yun, and Zhiyu Hao. 2018. Framework for risk assessment in cyber situation awareness. *IET Information Security* 13: 149–56. [CrossRef]
Yusgiantoro, Purnomo. 2014. Pedoman Pertahanan Siber, Peraturan Menteri Pertahanan Republik Indonesia, Jakarta. p. 14. Available online: https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf (accessed on 10 March 2022).
Zhou, Shicheng, Jingju Liu, Dongdong Hou, Xiaofeng Zhong, and Yue Zhang. 2021. Autonomous Penetration Testing Based on Improved Deep Q-Network. *Applied Science* 11: 8823. [CrossRef]