Ingénierie des Systèmes d'Information
Vol. 29, No. 1, February, 2024, pp. 205-218
Journal homepage: http://iieta.org/journals/isi

Risk Management Analysis of SMK Telkom Makassar's Integrated Academic Information System in Compliance with ISO 31000 Standards

Supriadi Sahibu[1*], Abdul Sakti[1], Akbar Iskandar[2]

[1] Department of Computer Systems, Universitas Handayani Makassar, Makassar 90231, Indonesia
[2] Department of Informatics, Universitas Teknologi Akba Makassar, Makassar 90245, Indonesia

Corresponding Author Email: supriadi@handayani.ac.id

https://doi.org/10.18280/isi.290121

Received: 7 May 2023
Revised: 10 July 2023
Accepted: 17 August 2023
Available online: 27 February 2024

Keywords:
Integrated Academic Information System (iGracias), SMK Telkom Makassar and information technology security

ABSTRACT

This investigation seeks to analyze the security risks associated with the Integrated Academic Information System (iGracias) application at SMK Telkom Makassar, using the ISO 31000 standards as a benchmark. The study employs the ISO 31000:2018 Information Technology Risk Management methodology, encompassing stages of risk identification, risk analysis, risk evaluation, and risk treatment. This methodology enables the researchers to ascertain that risks have been accurately identified, thoroughly analyzed, and appropriately mitigated, minimizing their potential impact on the organization. The findings reveal security issues in the iGracias application at SMK Telkom Makassar, identified through scanning with NMAP Kali Linux, which exposed several open ports, including port 21/tcp, port 22/tcp, and port 25/tcp. Consequently, these open ports present potential opportunities for unauthorized access and cyber-attacks. Moreover, the Mobile Security Framework (MobSF) test results yielded a Common Vulnerability Scoring System (CVSS) of 6.1, indicating a medium security level for the iGracias application in the Android environment. User responses revealed process risk at 84%, system security risk at 62%, and incidental risk at 57%. The outcomes of this investigation may serve as a guide in formulating and implementing strategies to uphold the security and quality of the applications in use.

1. INTRODUCTION

The advent of information technology has revolutionized educational landscapes, particularly in the realm of school administration and information management [1, 2]. However, this rapid technological advancement has invariably escalated the risks associated with its use in educational settings. It is therefore imperative for educational institutions to consistently undertake information technology risk management analyses to mitigate and minimize the adverse effects of these risks [3, 4].

The crux of information technology risk management in an educational context lies in safeguarding the systems and data from threats and untoward incidents, thereby ensuring their security [5]. The consequences of system security vulnerabilities can lead to unauthorized access and exposure of sensitive information, inflicting detrimental effects on institutions [6]. Despite the significance of system security awareness in thwarting cyber threats, empirical research on security risks in higher education and schools is scarce [7].

Potential information technology risks in schools may encompass data loss or leakage, virus and malware attacks, system hacking, and misuse of access [8, 9]. Consequently, a comprehensive risk management analysis is necessitated to identify, evaluate, and devise appropriate measures to attenuate or potentially eliminate these risks.

Robust information system security can avert financial loss, reputational damage, and severe academic system impairment [10]. Research has indicated a year-on-year increase in cyber attacks and security breaches in educational institutions, primarily attributed to lackadaisical attention to information security, ethical violations, and insufficient investment in security infrastructure [11, 12].

Risk management can play an instrumental role in maintaining the availability, integrity, and confidentiality of school data, and enhancing the efficacy of the learning process [13]. Regular risk management analysis activities can ensure the protection and safety of information technology systems and data, while minimizing potential losses resulting from unwanted information technology risks.

SMK Telkom Makassar utilizes the Integrated Academic Information System (iGracias) to streamline its administrative and academic activities. The iGracias Mobile Application facilitates real-time access to information such as class schedules, grades, attendance, announcements, and other academic information for students and parents, in addition to providing an online payment platform for school necessities. This application is envisaged to accelerate administrative processes, enhance efficiency, and simplify the monitoring of student academic progress (Figure 1).

Despite the pivotal role of iGracias in disseminating information throughout the academic community to support

all educational activities, system performance can be compromised by various hazards and risks. Therefore, a risk analysis of the iGracias information system is of paramount importance.

In Telkom Makassar Vocational School, it was discovered through observations that the system had never undergone a risk management analysis, rendering it susceptible to various attacks. These observations underscored the necessity for an information technology (IT) risk analysis using ISO 31000 risk management to mitigate and guard against potential threats.

Thus, this study aims to analyze information technology risk management in Integrated Academic Information Systems in schools using the ISO 31000 standard. The risks are stratified into very high, high, medium, low, and very low categories. Accordingly, a risk analysis of the Integrated Academic Information System (iGracias) at SMK Telkom Makassar is deemed essential.

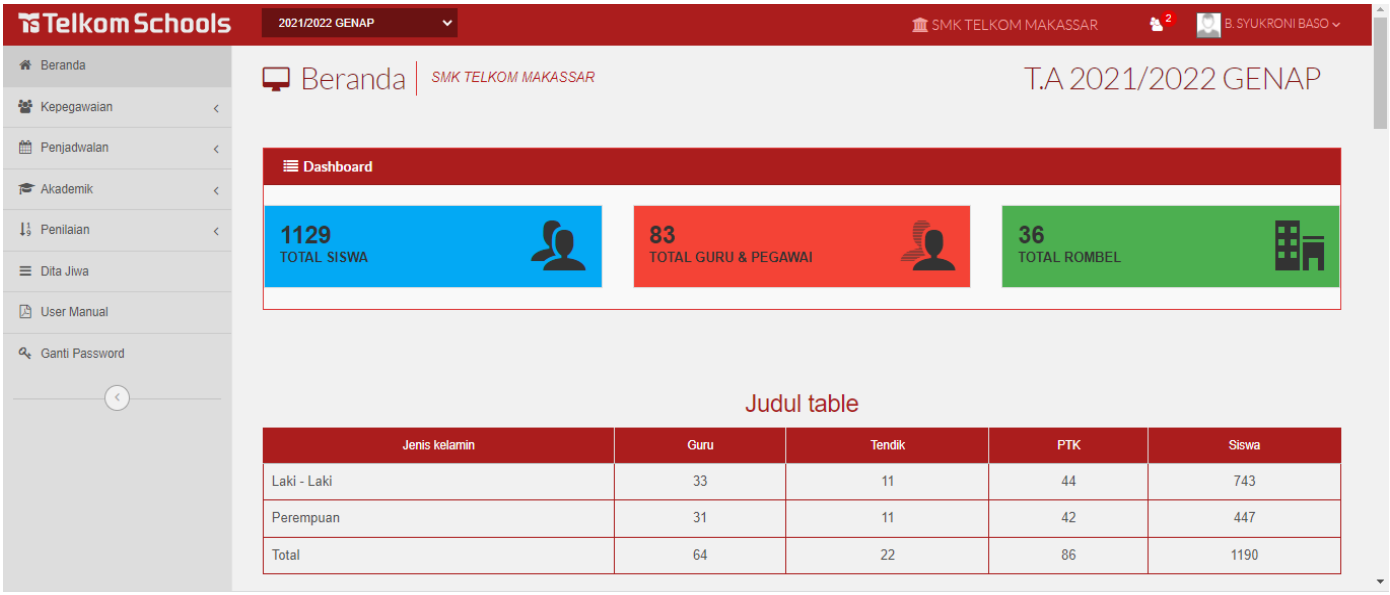


Figure 1. iGracias application dashboard

2. LITERATURE REVIEWS

2.1 Risk management analysis

The management of risk within information systems is a pivotal process that necessitates the identification, quantification, assessment, and mitigation of risks associated with the deployment of such systems within an organization [14]. An analysis is undertaken with the aim of pinpointing potential threats [15] and identifying inherent vulnerabilities in the existing information systems. Subsequently, it is the goal to devise suitable preventive or mitigation measures [16, 17]. Typically, the process involves a collaborative effort between the risk management and information technology teams to identify and address risks that may compromise the integrity of the information systems, such as data breaches or external attacks that can detrimentally affect both the users and the organization [18].

Such risks can manifest as data leaks, system damages, privacy infringements, and losses of IT assets, all of which can negatively impact the security and integrity of the information systems [19]. To prevent these adverse outcomes, it is essential to identify potential risks that may arise in every business process that involves IT. Upon identification, the subsequent step involves risk evaluation, wherein the likelihood and impact of the risk are assessed.

This evaluative process assists in determining the mitigation priority for the most critical risks. Methods of risk mitigation may encompass access management, routine system backups, IT usage activity monitoring, and periodic employee training on secure and non-harmful IT usage. Evaluations can be conducted internally through audit processes or externally through system penetration testing. Regular evaluations contribute to the enhancement of an organization's information system's quality and security [20]. In the digital era, IT risk management is considered a crucial component in ensuring business continuity, success, and integration at the business process level within an organization [21].

The efficacy of risk management hinges on its integration into corporate decision-making processes. The systematic and organized identification of risks that need to be managed by corporations is the objective of risk identification. This approach is vital as any undetected risks during this stage may be overlooked in the subsequent stages. Moreover, the procedure should focus on identifying risks that are within the organization's control. The ISO 31000 standard consists of six components: governance and commitment, integration, planning, implementation, assessment, and change [22, 23].

Risk assessment, as part of the risk assessment process, determines which risks require attention and their prioritization [24]. Risk analysis, which identifies the type and level of risk, assesses the potential impacts and risks an organization may encounter. Through the likelihood and impact matrix of IT risk management, organizations can take appropriate actions to curtail risks to their IT systems.

According to ISO 31000, risk is defined as the effect of uncertainty on objective achievement [25, 26]. Risk, as defined in the Big Indonesian Dictionary, is an unpleasant (dangerous) result of an action or activity. Conversely, the Australian Standard/New Zealand Standard 4360 2004 defines risk as a possibility that could influence a goal, measured by consequences and probabilities. While risk is often associated

with negative outcomes, accepting risk can also yield positive outcomes for companies, such as facilitating swift decisions to counteract cyberattacks [27].

2.2 Risk management principles

Principles of risk management pertaining to information technology encompass risk identification, assessment, control, and monitoring [28]. These principles form the bedrock of risk management, offering guidance in the formation and maintenance of structures and processes essential for risk management. The primary objective of these principles is to facilitate the accomplishment of organizational and corporate goals, thereby driving performance enhancement and innovation.

The International Organization for Standardization (ISO) has published ISO 31000, an international standard that provides guidelines for effective and efficient risk management [29]. This standard offers a versatile framework that can be adapted across diverse organizational types and industrial sectors. The principles of risk management delineated in ISO 31000 include:

a. Risk management should be a continuous, integrated process, consistently and systematically executed in alignment with the organization's business activities. This process requires regular monitoring and management.

b. Assessment of organizational context necessitates understanding the internal and external contexts that could engender risks, such as organizational objectives, market conditions, legal requirements, among others.

c. During the risk identification process, organizations should pinpoint risks that could potentially compromise their objectives. These risks can originate from various sources, including the work environment, technology, policies, procedures, and others.

d. Risk assessment by the organization entails evaluating the identified risks to determine their significance and the probability of their occurrence. Risk assessments should be data-driven and grounded in factual analysis.

e. In the risk treatment phase, organizations should decide on the appropriate strategy and actions to manage the identified and evaluated risks. Possible actions may include risk avoidance, risk monitoring, risk transfer, and others.

f. Organizations should ensure that effective communication and consultation is carried out with all stakeholders involved in risk-related matters, including employees, business partners, customers, and others.

g. Organizations must monitor and evaluate the efficacy of the risk management implemented, conducting regular risk assessments to ensure the identified risks remain relevant and congruent with the organization's context.

By implementing the risk management principles outlined in ISO 31000, organizations can enhance their risk management effectiveness and efficiency, bolstering their credibility and reputation among stakeholders. Compliance with the ISO 31000 standard also aids organizations in meeting the legal and regulatory requirements concerning risk management applicable in their region [30, 31].

2.3 Framework for risk management

The framework for risk management is designed to facilitate more effective risk management in institutions or businesses, serving as a reference for risk control and strategic planning [32, 33]. It is perceived that the success of risk management is contingent upon its integration into corporate decision-making processes. The framework, applied across various organizational levels and specific situations, fosters successful risk management by ensuring that risk information derived from the process is accurately reported and serves as the basis for accountability throughout the organization.

The ISO 31000 risk management framework outlines seven steps that organizations should follow to manage risk systematically and structurally [34]. The initial stage, evaluation, necessitates that organizations appraise and understand the risks associated with their operations. This is followed by the improvement stage where risks are assessed against specific criteria such as risk tolerance and organizational objectives. The third stage, integration, requires the development of a risk management strategy in line with the identified risk level.

The subsequent stage, design, involves the selection of suitable risk mitigation measures to address the identified risks. The following stage, implementation, mandates the execution of the selected risk management strategy. The penultimate stage, monitoring, calls for an evaluation of the effectiveness of the implemented risk management strategy. Lastly, the review stage involves periodic reassessments to ensure continued improvement of the risk management process. Adhering to all stages of the ISO 31000 risk management framework allows organizations to manage risks more effectively and minimize potential negative impacts on their operations.

The ISO 31000 risk evaluation matrix is utilized in risk management to assess risks identified by the organization [35]. This matrix aids organizations in the identification, assessment, and prioritization of operational risks. Within the ISO 31000 risk evaluation matrix, risk is analyzed based on two dimensions: the likelihood of risk occurrence and the resulting consequence or impact. Subsequently, the organization assigns a score to each dimension and combines them to attain an overall risk score. Two risk assessment methodologies exist, namely qualitative evaluation and quantitative evaluation, as illustrated in Figure 2.

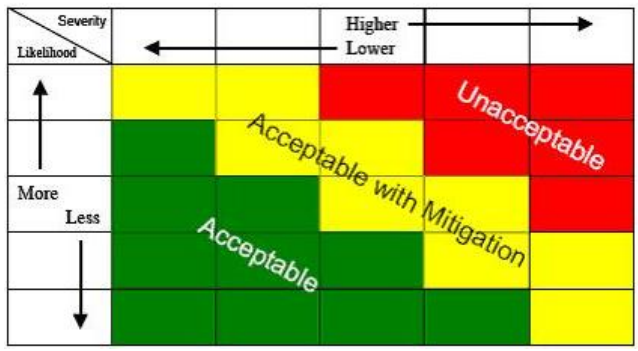


Figure 2. Risk evaluation matrix

3. METHODOLOGY

The research method used in this study uses the ISO 31000: 2018 method which begins with risk identification, risk analysis, risk evaluation, risk management [36-38]. The data analysis technique used is descriptive quantitative. The initial step taken in this study was to conduct interviews with iGracias information system operators with the aim of finding out how often an incident occurs that hinders activities in the

iGracias information system. In addition, using the Network Mapper (Nmap) and Mobile Security Framework (MobSF) tools to identify system security risks.

NMAP is a tool used to perform network scanning and find information about hosts connected to it, while Kali Linux is a Linux distribution specially designed for penetration testing and security testing [39]. Mobile Security Framework (MobSF) is a tool used to test the security of mobile devices [40]. In addition, research on Academic Information Systems Risk Management Analysis Using ISO 31000, NMAP, Kali Linux, and MobSF used to test the security of academic information systems in order to be able to perform tests on the system and identify potential security threats [41]. The results of this test can be used to carry out risk management, namely identifying potential damage that could occur and taking preventive action to address the identified risks.

Questionnaires are used to collect data through a series of questions or written statements to all respondents (users) to be answered directly [42], while the system eligibility criteria based on user responses use the risk probability criteria as shown in Table 1.

Next in Table 2, explains the risk impact criteria. Risk criteria are generally used to assist organizations in determining and evaluating the range of risks that will be taken or not taken in achieving a goal or target [14, 43]. Risk criteria should be determined and taken into consideration in light of the needs of the organization and the viewpoints of stakeholders. These risk criteria are dynamic and can be changed regularly if necessary.

Based on the previous explanation, Telkom Makassar Vocational School has now adopted an Integrated Academic Information System known as iGracias. However, iGracias does not yet have a risk identification system which will certainly affect the organization's goal of providing information to the entire academic community. So an information technology risk management plan is needed in accordance with the ISO 31000: 2018 standard. The information system risk management process can be seen in Figure 3, while the risk management flowchart for SMK Telkom Makassar can be seen in Figure 4.

Table 1. Risk probability criteria

Likelihood Rating	Probability	Probability (%)
1	Very rarely	0 - 10 %
2	Seldom	> 10% - 20%
3	Sometimes	>20% - 50%
4	Often	> 50% - 70%
5	Very often	>70%

Table 2. Risk impact criteria

Risk Rating	Criteria	Percent (%)	Description
1	Very small	0 - 30 %	Information system risk tends to be very low and the probability of being affected by a loss is very small.
2	Small	> 30% - 45%	Information system risk tends to be low and is likely to be impacted with little loss.
3	Intermediate	> 45% - 55%	Information system risk is likely to be moderate and likely to be adversely affected.
4	Big	> 55% - 70%	Information system risk tends to be high and the possibility of loss is very likely to occur.
5	Very large	>70%	Failure to achieve goals and failures.

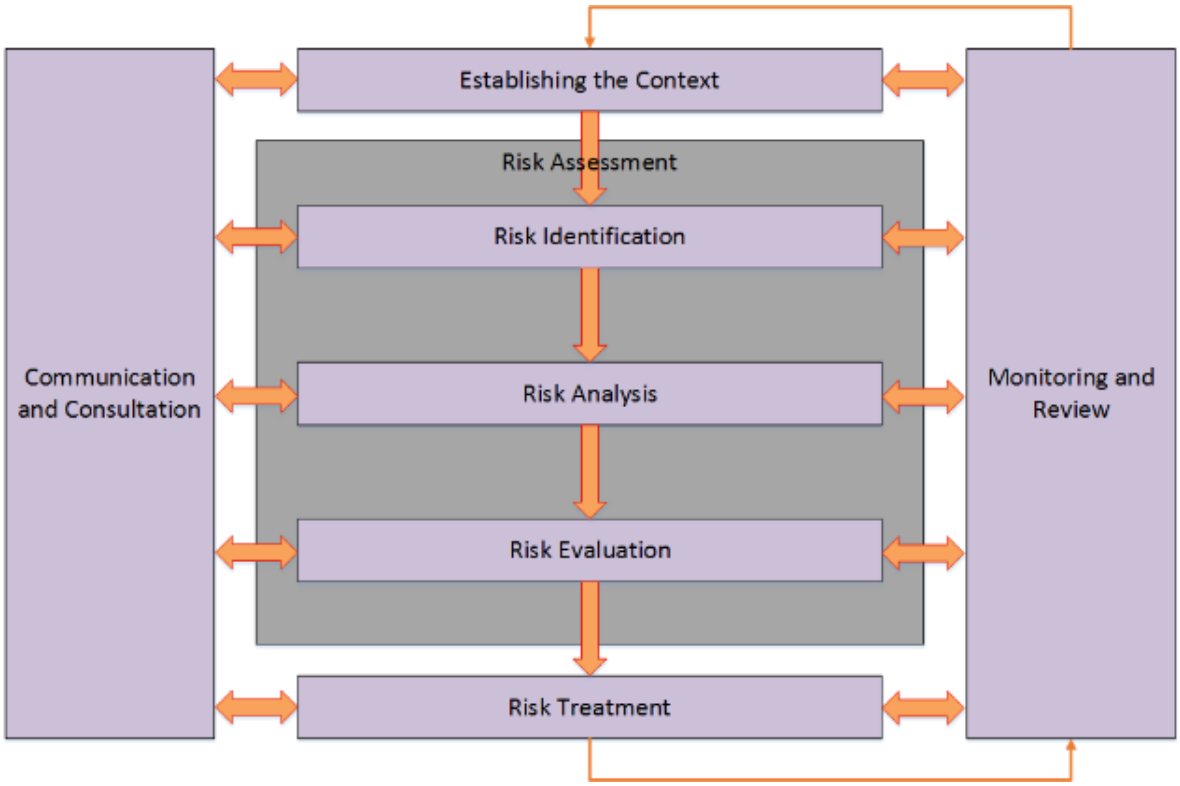


Figure 3. Information system risk management

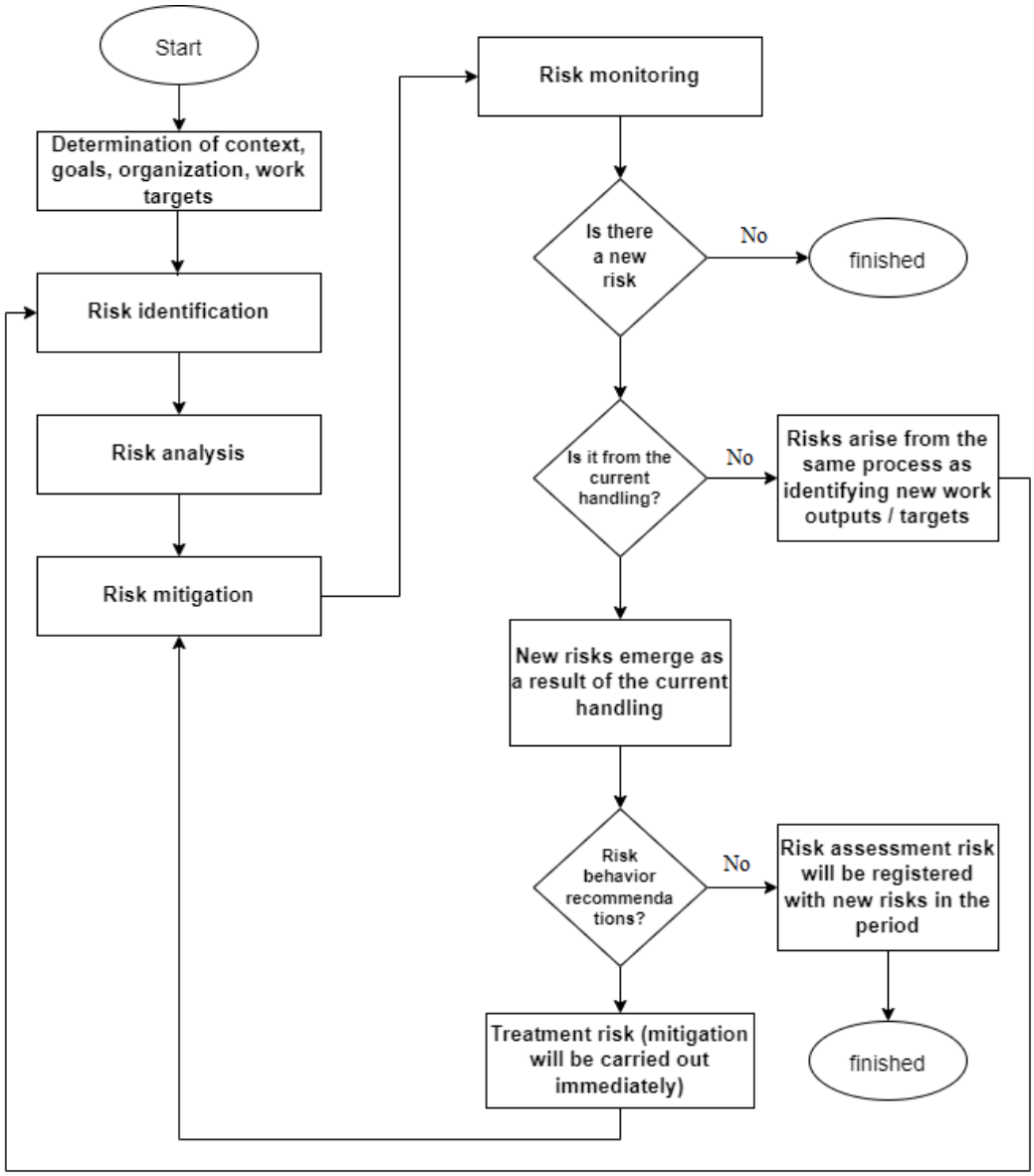


Figure 4. Flowchart of information system risk management analysis at SMK Telkom Makassar

4. RESULTS AND DISCUSSION

This section will explain the results of research on the analysis of information technology risk management on the iGracias information system at SMK Telkom Makassar, while the stages in risk management planning are risk identification, risk analysis, risk evaluation, risk treatment [44]. The risk management process according to ISO 31000 is as follows:

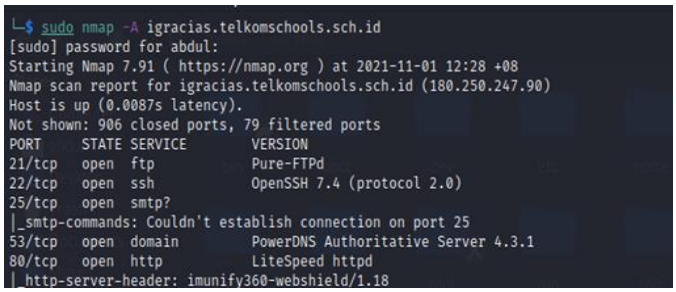
a. Communication: Consultation and communication with stakeholders to assist the process of investigation and assessment of the system.
b. Determination of Context: Context intended to describe the basis of risk management, as well as boundaries and criteria.
c. Risk Assessment: Risk assessment is described by ISO 31000 as a general process of risk identification, analysis and evaluation.

Based on the stages, the first step taken is to identify possible risks that might occur by the scanning method using the Mobile Security Framework (MobSF), NMAP Kali Linux and a questionnaire for system user responses.

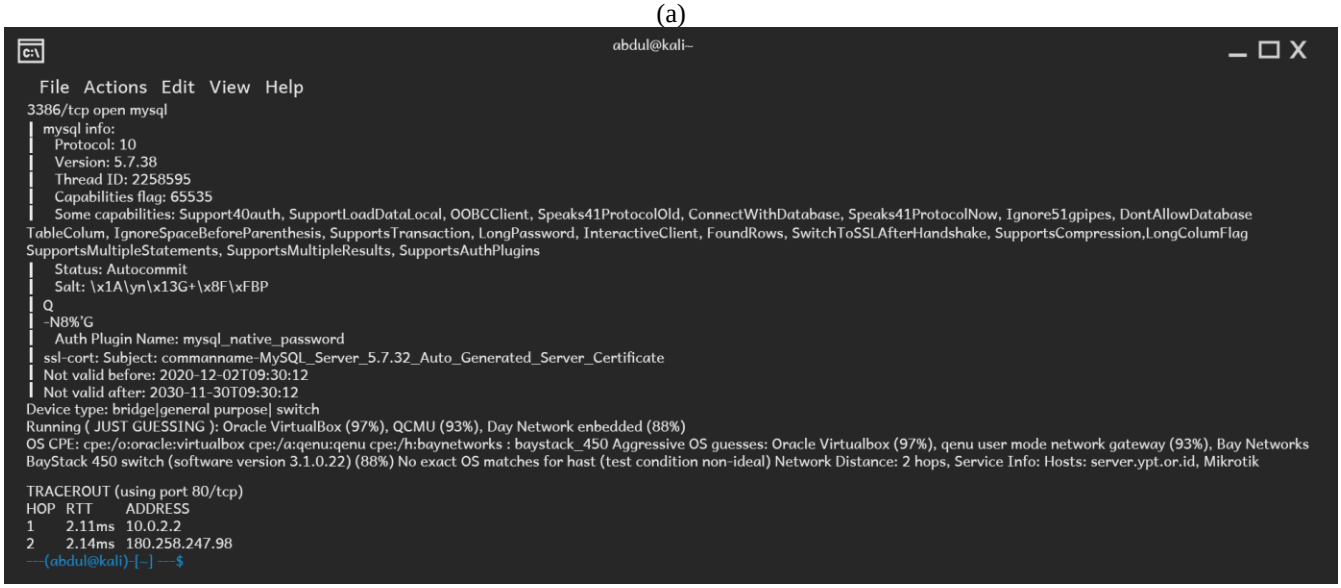
4.1 Risk identification

The purpose of risk identification in this study is a process to capture any risks that have the potential to hinder the achievement of the goals and objectives of the iGracias information system at SMK Telkom Makassar. Based on the results of scanning using Nmap on the Kali Linux terminal by giving the command "nmap -A iGracias.telkomsel.sch.id" information was obtained that several ports on the iGracias system were open, such as port 21/tcp, port 22/tcp, port 25/ tcps and others. This can provide information that the port can pose a risk of infiltration, exploitation, data theft and the spread of malware in the academic information system of SMK Telkom Makassar. The results of the analysis can be seen in Figure 5.

The -A option in the command above aims to perform an aggressive scan by activating several options automatically such as detecting the operating system used by the host, the software version used, running several scripts related to the destination host and tracing network routes. While the results of identification of possible risks with the Mobile Security Framework (MobSF) can be seen in Figure 6.



(a)



(b)

Figure 5. Scanning results using Nmap

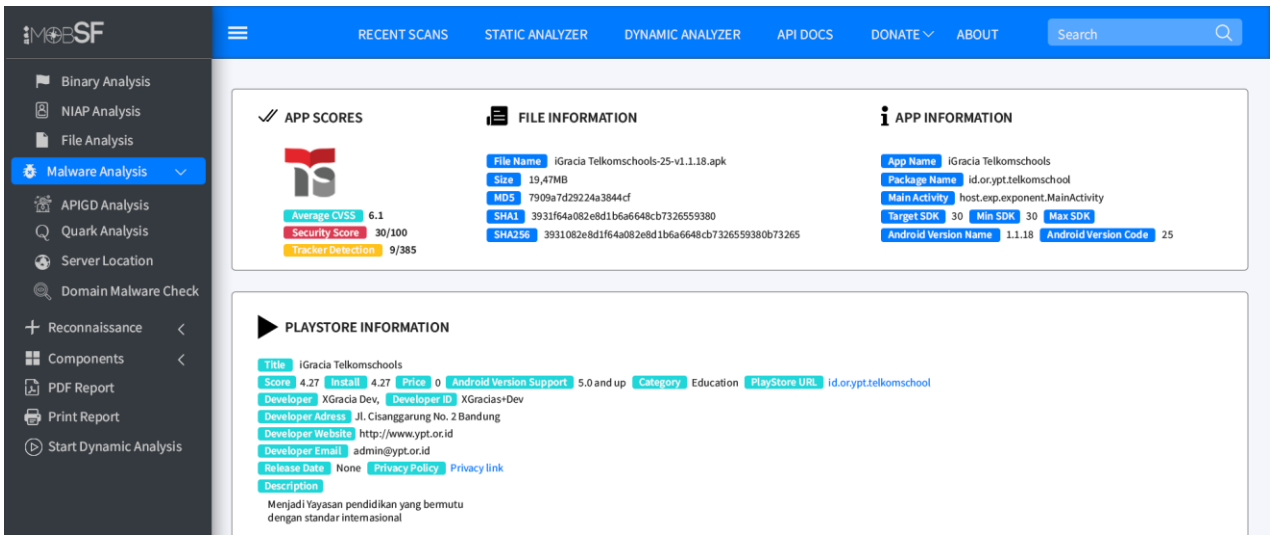


Figure 6. Scanning results using MobSF

Table 3. Process risk identification

Risk Code	Process Risk Type	Yes		No	
		∑	%	∑	%
R001	Abuse of access rights	20	80	5	20
R002	Device theft	17	68	8	32
R003	Limited access bandwidth	23	92	2	8
R004	Failure to enter data	24	96	1	4
R005	There is no regular hardware maintenance	25	100	-	-
R006	Staff concurrent other tasks	20	80	5	20
R007	Server down	24	96	1	4
R008	Database errors	16	64	9	36

Table 4. iGracia system security risk identification

Risk code	Types of System Security Risks	Yes		No	
		∑	%	∑	%
R009	Network hacking	15	60	10	40
R010	Infected with malware	20	80	5	20
R011	Vulnerabilities	16	64	9	36
R012	SQL injections	14	56	11	44
R013	Cross script scripting (XSS)	13	52	12	48

Table 5. Incidental risk identification

Risk Code	Incidental Risk Type	Yes		No	
		∑	%	∑	%
R014	Flood	13	52	12	48
R015	Lightning	14	56	11	44
R016	Earthquake	16	64	9	36

The Mobile Security Framework (MobSF) is a framework used for testing mobile applications that is capable of automatically analyzing the vulnerabilities or security holes of an application either on the Android, IOS or Windows operating system. Based on the results of the Application Package (APK) scanning on the iGracias android application using MobSF tools, an Averange CVSS (Common Vulnerability Scoring System) value of 6.1 means that the security level of the iGracias application is in the medium category, so that the risk of illegal access to the iGracias application can still occur.

Based on risks that have been identified with previous MobSF and NMAP tools. Furthermore, identification of risks with the questionnaire method involving all staff and teachers who use the igraicas information system. In this study there are sixteen types of risk. Front types of risk identification can be seen in Table 3.

Based on Table 3, an average process risk value of 84% is obtained for each type of risk faced, namely risk code R001 concerning abuse of access rights. At this risk it appears that 80 percent of respondents stated that the system was used by people who were not responsible, while 20 percent said they were not. Furthermore, the risk code R002 (device theft) means operational loss risk, because 68 percent of respondents chose Yes and 32 percent of respondents chose No. Risk code R003 (Bandwidth access limited) the risk that will occur causing access failure to the information system based on the information of respondents 92 percent chose Yes and 8 percent chose No.

Risk code R004 (data input error) describes an error in data input resulting in an invalid report. Based on the risk instrument code, it was obtained that 96 percent of respondents chose "Yes" which means the risk of invalid process or data was caused by errors in data input and 4 percent of respondents stated that there was no problem. Risk code R005 (no hardware maintenance) can cause more severe damage and this was agreed upon by respondents as evidenced by the responses of 100 percent of respondents choosing "yes" and this has never been done hardware maintenance on the iGracias system of SMK Telkom Makassar.

Risk code R006 (staff concurrently with other duties) risks that can occur due to neglect of the main task due to additional tasks, this is evidenced by the response of respondents by 80 percent choosing "Yes" to do other tasks or additional tasks while 20 percent chose "no". In addition, server down and database errors often occur. In addition to identifying process risks, there are also threat risks, which can be seen in Table 4.

Table 4 describes the iGracias information system security risk with an average security risk value of 62%. As for the recapitulation of respondents' answers based on risk code R009 (hacking of networks), information was obtained that 60 percent of respondents agreed or chose "yes" if the system would be at risk of being damaged if an intruder took advantage of the security hole for his personal interests and 40 percent of respondents chose No risk. Furthermore, for the risk code R010 (attacked by malware), information was obtained that 80 percent of respondents stated that if the system was attacked by malware, it would have an impact on data damage and even data loss, while 20 percent said no. Additionally, for risk code R011 (vulnerability), R012 (SQL Injection) and R013 (cros script scripting) also provide information that the security of the system is vulnerable to intruders taking over the iGracias information system. This causes the importance of identifying system security risks. Further incidental risk identification was carried out through the responses of respondents as shown in Table 5.

Table 5 describes the risks caused by natural disasters, an average value of 57% is obtained with an explanation of each type of incidental risk, namely the risk code R014 (flood) provides information that 52 percent of respondents stated that the iGracias system is vulnerable to the impact of flooding which causes losses either in information system infrastructure or other material losses and 48 percent of respondents stated that they did not have incidental risks. Furthermore, for risk code R015 (lightning) explaining about natural disasters caused by lightning or natural phenomena providing information if 56 percent of respondents stated that the risk of lightning had the opportunity to disrupt the iGracias system of SMK Telkom Makassar and 44 percent stated that there was no risk of damage caused by lightning.

4.2 Risk analysis

Risks that have been previously identified with several methods, then carried out a risk analysis with two criteria, namely the probability criteria and the impact criteria. The probability criterion explains how often the risk will occur, while the impact criterion explains how big the consequences will be if the risk occurs. In the risk analysis in this study using the questionnaire method with the aim of knowing the value of the probability and impact on a risk based on the assessment of each respondent. The results of process risk analysis, security threat risk analysis and incidental risk analysis results can be seen in Tables 6-8.

Based on the results of the analysis in Table 6, it can be seen that the average number of probabilities for abuse of access rights is 0.52 and the impact value is 0.64. So the probability likelihood rating is at level four (often) and the risk rating is at level four (high risk), which means that the problems faced by an organization tend to be high and there is a high probability of loss. Device theft has an average probability of 0.44 and an impact value of 0.60. The probability value is at the likelihood rating level (sometimes) and the impact value is at level four (high risk). Furthermore, the probability for limited access bandwidth, negligence in data input data and database errors is at the likelihood rating level four (often), while the impact value of limited access bandwidth.

Furthermore, the probability value for this type of risk is explained because there is no periodic hardware maintenance, Staff concurrently working on other tasks and server down is in the category of probability (sometimes), while the impact value due to the absence of periodic hardware maintenance, staff concurrently other duties has a risk rating level one (very small) and due to server down has a risk rating level five (very large) which means that a goal is not achieved and there is only failure.

Table 6. Results of process risk analysis

Risk Code	Process Risk Type	Probability	Impact
R001	Abuse of access rights	0.52	0.64
R002	Device theft	0.44	0.60
R003	Limited access bandwidth	0.52	0.44
R004	Data input negligence	0.56	0.35
R005	There is no regular hardware maintenance	0.32	0.24
R006	Staff concurrent other tasks	0.28	0.24
R007	Server down	0.40	0.80
R008	Database errors	0.52	0.92

Table 7. Results of security threat risk analysis

Risk Code	Risk type	Probability	Impact
R009	Network hacking	0.40	0.68
R010	Infected with malware	0.40	0.52
R011	Vulnerabilities	0.48	0.76
R012	SQL injections	0.44	0.56
R013	Cross script scripting (XSS)	0.32	0.64

Table 8. Incidental risk analysis results

Risk Code	Risk type	Probability	Impact
R014	Flood	0.20	0.48
R015	Lightning	0.16	0.72
R016	Earthquake	0.8	0.28

Table 7 describes the results of the risk analysis of information system security threats at SMK Telkom Makassar with an average probability of hacking a network of 0.40, while the chance of being attacked by malware (0.40), Vulnerability (0.48), SQL injection (0.44)), Cross script scripting (0.32). This value illustrates the probability likelihood rating is at level three (sometimes) and the value of the impact of hacking on the network is (0.68), SQL injection (0.56), Cros script scripting (0.64) at level four (high risk)) which means the risk to the information system of SMK Telkom Makassar tends to be high and the possibility of loss is very likely to occur. Likewise, the Vulnerability impact value of (0.76) is at level five (very large impact), which means it can causenot achieving the target. While the value of the impact caused by malware is at level three (medium risk impact) with a value of 0.52 which means the risk faced by organizations caused by malware tends to be moderate and is likely to be adversely affected.

Referring to Table 8, it appears that the average probability value caused by flooding is obtained by a value of 0.20 and the probability value of lightning risk is obtained by a value of 0.16 with an likelihood rating level four (rare), then for the probability value caused by an earthquake of 0.8 on the likelihood rating level four (very rare). Meanwhile, the value of the impact of flooding is at level three (medium) with an impact value of 0.48, meaning that the risks faced by the organization/information system tend to be moderate and may be adversely affected. Moreover, the type of lightning risk is at level five (very large) with a value of 0.72 which means that lightning risk can affect the achievement of an organizational goal.

After obtaining the results of the risk probability weights and the risk impact weights of the iGracias information system, risk mapping is then carried out using the calibration method based on the probability table and risk impact as shown in Figure 7.

The matrix in Figure 7 shows which risks are included in the red zone risk (high risk), yellow zone (medium risk) and green zone (low risk). The risks that fall into the red zone (high risk) include risks with codes R001 (abuse of access rights), R007 (server down), R008 (database error) and R011 (vulnerability). Furthermore, for the yellow zone (moderate), namely risk with code R002 (device theft), R003 (bandwidth access limited), R004 (moderate) negligence in data input, R009 (hacking), R012 (SQL injection), R013 cross script scripting (XSS), R010 (attacked by malware), R15 (lightning) while low risk there are four risks with the code R006 (staff concurrently serving other duties), R005 (no maintenance), R014 (flood), R0016 (earthquake).

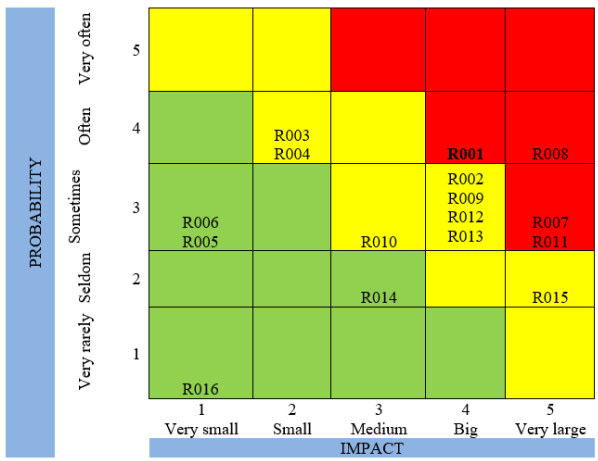


Figure 7. Risk evaluation matrix

4.3 Risk evaluation

Risk evaluation or risk assessment on information systems is an important step in information security management. One of the methods that can be used in conducting a risk evaluation is based on the risk score and risk ranking. The risk score is an assessment of the level of potential risk that is calculated based on two factors, namely the likelihood or likelihood of a risk

occurring and the impact caused by that risk. In calculating the likelihood, an analysis is carried out on how likely the risk is to occur, while in calculating the impact, an analysis is carried out on how much impact will result if the risk occurs.

Table 9. Risk evaluation

Risk Code	Risk	Risk Score	Ranking Risk
R001	Abuse of access rights	16	2
R002	Device theft	12	7
R003	Limited access bandwidth	8	11
R004	Data input negligence	8	12
R005	There is no regular hardware maintenance	3	14
R006	Staff concurrent other tasks	3	15
R007	Server down	15	3
R008	Database errors	20	1
R009	Network hacking	12	8
R010	Infected with malware	9	10
R011	Vulnerabilities	15	4
R012	SQL injections	12	5
R013	Cross script scripting(xss)	12	6
R014	Flood	6	13
R015	Lightning	10	9
R016	Earthquake	1	16

After the risk score is calculated, the risk ranking is determined. Risk ranking is a tool used to prioritize which risks must be addressed first and risk ranking is determined by comparing the risk score of one risk with another. The higher the risk score of a risk, the higher its position in the risk ranking. So risk evaluation aims to see risks that have the highest value and occur frequently. Based on these objectives, steps are taken to sort the highest risk to the lowest risk as shown in Table 9.

The results of the risk evaluation in Table 9 are determined by assessing the risk based on the risk score obtained from the multiplication of the impact and probability from the matrix table, while the risk ranking is determined by sorting the risk score from the highest value to the lowest. From the results of the risk evaluation, it can be seen that the risk included in the high risk category is code R008 (database error) with the highest score of 20. This score is in accordance with the findings in the operation of the iGracias information system database system as shown in Figure 8, followed by the risk of abuse of access rights with a risk score of 16, as well as server down and vulnerability, each of which has a risk score of 15.

4.4 Risk treatment

Risk treatment of information systems is a process to reduce or eliminate risks associated with information systems in an organization. This process is carried out by identifying and evaluating existing risks, then taking appropriate actions to reduce the impact that can occur when these risks occur. There are several types of actions that can be taken in risk treatment, including transferring risks to third parties, avoiding risks, reducing risks, and tolerating risks. The action chosen depends on the nature and level of risk. Risk Treatment is one way to ensure that information systems within an organization are always safe and protected from threats that may occur.

Based on the results of the previous risk evaluation, we can determine which risks will be handled first and immediately, so that treatment is needed as a step to carry out a risk response as explained below:

Process Risk

Risk code R001

Risk type: Abuse of access rights

Risk response:

- Limiting users in accessing the information system
- Assign users to those with responsibility

Deactivate the user id of users who have left the organization

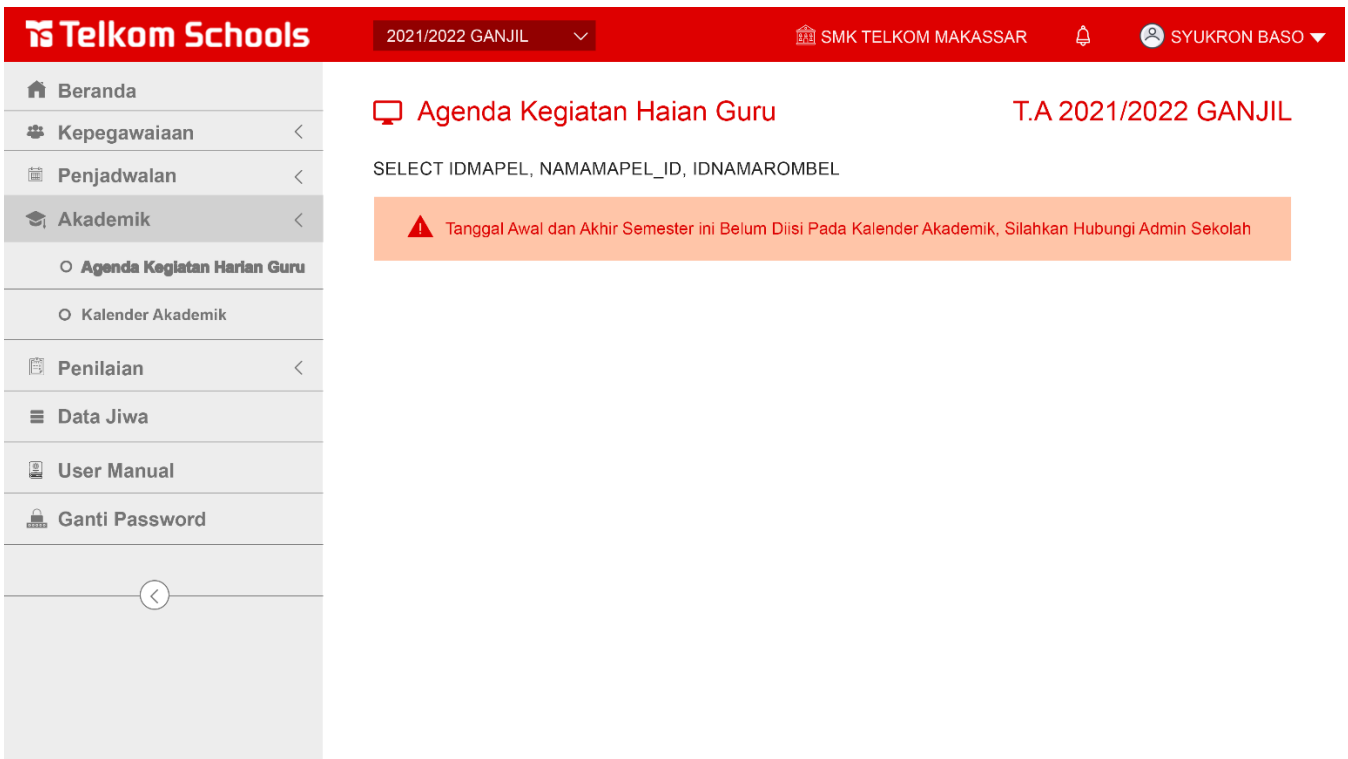


Figure 8. Database errors

Risk code R002
Risk type: Device theft
Risk response: Installation of CCTV and monitoring systems
Risk code R003
Type of risk: Bandwidth access limited
Risk response:
- Make a schedule in accessing the information system
- Increase network bandwidth
- Optimizing program logic or database queries

Risk code R004
Risk type:
Negligence to enter data in the information system
Risk response:
SOP is required for re-checking data that has been entered
Risk code R005
Risk type:
Absence of regular hardware repairs
Risk response:
A regular hardware maintenance schedule is required
Risk code R006
Type of risk: Staff concurrently on other assignments
Risk response: Recruit new employees and provide training
Risk code R007
Risk type: Server down
Risk response:
It is very important to check the server regularly and have a maintenance schedule and provide information to users before the server is shut down
Risk code R008
Risk type: Database error
Risk response:
- Repairing corrupted databases
- Check database login credentials
- Repair corrupted files
- Perform regular database backups
- Delete obsolete data

Security Threat Risk
Risk code R009
Type of risk: Hacking against the network
Risk response:
- Perform network security monitoring connected with unknown access
- Provides protection/firewel protection

Risk code R010
Risk type: Vulnerability
Risk response:
Perform Vulnerability Assessments and Penetration Tests
Risk code R011
Risk type: Malware virus attack
Risk response:
- Setting up anti-virus malware detection/detection
- Install/update software regularly

Risk code R012
Risk type: SQL injection
Risk response:
- Filter input validation, especially the use of single quotes
- Hide error messages from a running SQL server
- If possible, disable standard features such as broken procedures
- On the [SQL Server Security] tab, change startup to run SQL Server as a low privilege user
- Installing a Web Application Firewall (WAF) and Intrusion Prevention System (IPS)

Risk code R013
Risk type: Cross script scripting (XSS)
Risk response:
- Using XSS prevention libraries such as PHP anti XSS, HTML Purifier, XSS HTML filter
- Using SDL in web applications can help reduce coding errors and avoid XSS attacks.

Incidental Risk
Risk code R014
Risk type: Flood
Risk response: Acceptance
Risk code R015
Risk type: Lightning
Risk response: Acceptance
Risk code R016
Risk type: Earthquake
Risk response: Acceptance

Information technology has now become a very important part of human life [45]. Likewise in the world of education, information technology is an important part of supporting learning activities and school administration [46, 47]. However, the use of information technology also presents various risks that must be managed properly so as not to disrupt the smooth learning process and school administration. Therefore, an analysis of school information technology risk management using ISO 31000:2018 is very important to do.

In general, these risks can be divided into several types and have different levels of risk. However, sometimes not all risks can be overcome at once, so it is necessary to prioritize them in handling them. In this case, the author explained that we can determine which risks need to be addressed first and immediately. This can be done based on the problem being faced and by carrying out the right handling or treatment. Thus, information system security risks can be minimized and information system security can be maintained properly.

Prioritization of risk management cannot only be based on the problem being faced, but also considers several factors that can affect the level of risk and the impact of these risks. These factors include the frequency of risk occurrence, the value of assets affected by the risk and potential losses that may occur. In this case, a good information system security risk evaluation must also be carried out continuously. Along with technological developments and increasingly complex attack methods, information system security risks are also increasingly diverse and changing. Therefore, it is necessary to carry out periodic risk evaluations to ensure that information system security is maintained and risks can be handled appropriately.

This study identifies the risks that can occur in information technology systems in schools through risk identification, risk analysis, risk evaluation and risk management. In the risk identification stage, researchers identified several risks that might occur in information technology systems in schools such as data leakage, data loss, computer virus attacks, and security system vulnerabilities. Then, in the risk analysis stage, the researcher conducts an assessment of the possibility of a risk occurring and the impact that can arise from that risk. After that, a risk evaluation is carried out by considering the level of possibility and impact of the risk.

The results of the study show that some risks have a high degree of probability and impact, such as data leaks and security system vulnerabilities caused by database errors,

abuse of access rights, server downtime and vulnerabilities. Handling risks, researchers provide recommendations for implementing several actions such as increasing network security, protecting important data, and managing user access rights. In addition, it is also recommended to carry out training and development of human resources in the field of information technology in order to be able to minimize risks.

So by doing good risk management, schools can anticipate or minimize the risks that might occur. So that risk management carried out using the ISO 31000: 2018 standard helps in strengthening risk management in information technology systems in schools, so that it can become a reference for school institutions in improving the quality of risk management in their information technology systems, especially SMK Telkom Makassar. So by carefully evaluating the impact of risks, schools can improve systems, improve security and protect sensitive data. This is also explained by [48, 49] that with good risk management can have a positive impact on the sustainability of the company, especially the positive impact on the information system owned by an organization. This was disclosed because various problems could have occurred for the company so it was necessary to review and evaluate at any time to avoid unwanted things, such as misuse of access rights by illegal means [50].

5. CONCLUSIONS

Based on the results of the analysis and previous discussion, it can be concluded that the ISO 31000:2018 method can provide information about risk response to help manage iGracias information technology (IT) risks. Furthermore, from the results of the risk identification, risk information is obtained regarding abuse of access rights, device theft, limited access bandwidth, negligence in inputting data, no regular hardware maintenance, staff concurrently working on other tasks, server down, database errors, network hacking, viruses. malware and SQL injection. Furthermore, there are four high level risks, namely access rights abuse, server down, database errors and vulnerabilities, while eight moderate level risks (limited bandwidth access, negligence in data input, device theft, hacking, SQL injection, cross scrip scripting, lightning), as well as four low level risks (no regular maintenance, staff concurrently doing other tasks, floods, earthquakes). So using the ISO 31000: 2018 method can help the school anticipate the risk of failure of the academic information system at school.

Therefore, further researchers are expected to conduct research in the field of risk management analysis specifically for information system infrastructure and compare risk management between schools in Indonesia.

ACKNOWLEDGMENT

Acknowledgments to all colleagues for supporting this research, especially to the Chancellor of Universitas Handayani Makassar and the principal and teachers of SMK Telkom Makassar for their willingness to provide data to us.

REFERENCES

[1] Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., Kundi, G.S. (2021). Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. Technology in Society, 65: 101565. https://doi.org/10.1016/j.techsoc.2021.101565

[2] Martins, J., Branco, F., Gonçalves, R., Au-Yong-Oliveira, M., Oliveira, T., Naranjo-Zolotov, M., Cruz-Jesus, F. (2019). Assessing the success behind the use of education management information systems in higher education. Telematics and Informatics, 38(1): 182-193. https://doi.org/10.1016/j.tele.2018.10.001

[3] Meland, P.H., Nesheim, D.A., Bernsmed, K., Sindre, G. (2022). Assessing cyber threats for storyless systems. Journal of Information Security and Applications, 64: 103050. https://doi.org/10.1016/j.jisa.2021.103050

[4] Iskandar, A., Kartowagiran, B., Haryanto, H., Suyanto, S., Mustapa, M., Munawir, M. (2023). Web based tolada village information system design. TEM Journal, 12(1): 334-340. https://doi.org/10.18421/TEM121-42

[5] Ayaburi, E.W. (2023). Understanding online information disclosure: examination of data breach victimization experience effect. Information Technology & People, 36(1): 95-114. https://doi.org/10.1108/ITP-04-2021-0262

[6] Wu, A.Y., Hanus, B., Xue, B., Mahto, R.V. (2023). Information security ignorance: An exploration of the concept and its antecedents. Information & Management, 103753. https://doi.org/10.1016/j.im.2023.103753

[7] Ulven, J.B.U., Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2): 39. https://doi.org/10.3390/fi13020039

[8] Szczepaniuk, E.K., Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. Telecommunications Policy, 46(3): 102282. https://doi.org/10.1016/j.telpol.2021.102282

[9] Nottingham, E., Stockman, C., Burke, M. (2022). Education in a datafied world: Balancing children's rights and school's responsibilities in the age of Covid 19. Computer Law & Security Review, 45: 105664. https://doi.org/10.1016/j.clsr.2022.105664

[10] Farid, G., Warraich, N.F., Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010-2022). Journal of Information Science, 01655515231160026. https://doi.org/10.1177/01655515231160026

[11] Aslan, Ö., Aktug, S.S., Ozkan-Okay, M., Yilmaz, A.A., Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6): 1333. https://doi.org/10.3390/electronics12061333

[12] Li, H., Yoo, S., Kettinger, W.J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. Journal of Management Information Systems, 38(1): 222-245. https://doi.org/10.1080/07421222.2021.1870390

[13] Shiau, W.-L., Wang, X., Zheng, F. (2023). What are the trend and core knowledge of information security? A citation and co-citation analysis. Information & Management, 60(3): 103774. https://doi.org/10.1016/j.im.2023.103774

[14] Alejandro, M.C., Andrés, G.H., Ricardo, V.F. (2023). Constructing an architecture-based cybersecurity solution for a system. MethodsX, 102010. https://doi.org/10.1016/j.mex.2023.102010

[15] Qamar, S., Anwar, Z., Afzal, M. (2023). A systematic

threat analysis and defense strategies for the metaverse and extended reality systems. Computers & Security, 103127. https://doi.org/10.1016/j.cose.2023.103127

[16] Mouratidis, H., Islam, S., Santos-Olmo, A., Sanchez, L. E., Ismail, U.M. (2023). Modelling language for cyber security incident handling for critical infrastructures. Computers & Security, 128: 103139. https://doi.org/10.1016/j.cose.2023.103139

[17] Rahman, M.H., Wuest, T., Shafae, M. (2023). Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies. Journal of Manufacturing Systems, 68: 196–208. https://doi.org/10.1016/j.jmsy.2023.03.009

[18] Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management. Journal of Information Security and Applications, 73: 103433. https://doi.org/10.1016/j.jisa.2023.103433

[19] Bernsmed, K., Bour, G., Lundgren, M., Bergström, E. (2022). An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects. Journal of Air Transport Management, 102: 102223. https://doi.org/10.1016/j.jairtraman.2022.102223

[20] Xu, J., Liu, Z., Wang, S., Zheng, T., Wang, Y., Wang, Y., Dang, Y. (2022). Foundations and applications of information systems dynamics. Engineering. https://doi.org/10.1016/j.eng.2022.04.018

[21] Kechagias, E.P., Chatzistelios, G., Papadopoulos, G.A., Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection, 37: 100526. https://doi.org/10.1016/j.ijcip.2022.100526

[22] Banowosari, L.Y., Gifari, B.A. (2019). System analysis and design using secure software development life cycle based on ISO 31000 and STRIDE. Case study mutiara ban workshop. In 2019 Fourth International Conference on Informatics and Computing (ICIC), pp. 1-6. https://doi.org/10.1109/ICIC47613.2019.8985938

[23] Willumsen, P., Oehmen, J., Stingl, V., Geraldi, J. (2019). Value creation through project risk management. International Journal of Project Management, 37(5): 731-749. https://doi.org/10.1016/j.ijproman.2019.01.007

[24] Talari, G., Cummins, E., McNamara, C., O'Brien, J. (2022). State of the art review of Big Data and web-based Decision Support Systems (DSS) for food safety risk assessment with respect to climate change. Trends in Food Science & Technology, 126: 192–204. https://doi.org/10.1016/j.tifs.2021.08.032

[25] Reniers, G., Landucci, G., Khakzad, N. (2020). What safety models and principles can be adapted and used in security science? Journal of Loss Prevention in the Process Industries, 64: 104068. https://doi.org/10.1016/j.jlp.2020.104068

[26] Masso, J., Pino, F.J., Pardo, C., Garcia, F., Piattini, M. (2020). Risk management in the software life cycle: A systematic literature review. Computers, Standards & Interfaces, 71: 103431. https://doi.org/10.1016/j.csi.2020.103431

[27] Giuca, O., Popescu, T. M., Popescu, A.M., Prostean, G., Popescu, D.E. (2021). A survey of cybersecurity risk management frameworks. In Soft Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018), I8: 240-272. https://doi.org/10.1007/978-3-030-51992-6_20.

[28] Kwateng, K.O., Amanor, C., Tetteh, F.K. (2022). Enterprise risk management and information technology security in the financial sector. Information and Computer Security, 30(3): 422-451. https://doi.org/10.1108/ICS-11-2020-0185

[29] Rampini, G.H.S., Takia, H., Berssaneti, F.T. (2019). Critical success factors of risk management with the advent of ISO 31000 2018-Descriptive and content analyzes. Procedia Manufacturing, 39: 894-903. https://doi.org/10.1016/j.promfg.2020.01.400

[30] Andersen, T.J., Sax, J., Giannozzi, A. (2022). Conjoint effects of interacting strategy-making processes and lines of defense practices in strategic risk management: An empirical study. Long Range Planning, 55(6): 102164. https://doi.org/10.1016/j.lrp.2021.102164

[31] Sánchez-Garcia, I.D., Gilabert, T.S.F., Calvo-Manzano, J.A. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. Computers & Security, 128: 103170. https://doi.org/10.1016/j.cose.2023.103170

[32] Kure, H.I., Islam, S., Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 34(18): 15241-15271. https://doi.org/10.1007/s00521-022-06959-2

[33] Razikin, K., Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Egyptian Informatics Journal, 23(3): 383-404. https://doi.org/10.1016/j.eij.2022.03.001

[34] Pandithawatta, S., Ahn, S., Rameezdeen, R., Chow, C. W. K., Gorjian, N., Kim, T.W. (2023). Development of a knowledge graph for automatic job hazard analysis: The schema. Sensors, 23(8): 3893. https://doi.org/10.3390/s23083893

[35] Wiradarma, A. A. B. A., & Sasmita, G. M. A. (2019). IT risk management based on ISO 31000 and OWASP framework using OSINT at the information gathering stage (Case Study: X Company). International Journal of Computer Network and Information Security, 10(12): 17. https://doi.org/10.5815/ijcnis.2019.12.03

[36] Kheir, O., Jacoby, A., Verwulgen, S. (2022). risk identification and analysis in the development of medical devices among start-ups: Towards a broader risk management framework. Medical Devices: Evidence and Research, 15: 349-363. https://doi.org/10.2147/MDER.S375977

[37] Canedo, E.D., do Vale, A.P.M., Gravina, R.M., et al. (2022). ICT governance and management macroprocesses of a brazilian federal government agency. Information, 13(5): 231. https://doi.org/10.3390/info13050231

[38] Lu, L., Kujala, P., Kuikka, S. (2022). On risk management of shipping system in ice-covered waters: Review, analysis and toolbox based on an eight-year polar project. Ocean Engineering, 266: 113078. https://doi.org/10.1016/j.oceaneng.2022.113078

[39] Tudosi, A.-D., Graur, A., Balan, D.G., Potorac, A.D. (2023). Research on security weakness using penetration

testing in a distributed firewall. Sensors, 23(5): 2683. https://doi.org/10.3390/s23052683
[40] Bokolo, B., Sur, G., Liu, Q., Yuan, F., Liang, F. (2022). Hybrid analysis based cross inspection framework for android malware detection. In 2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA), Las Vegas, NV, USA, pp. 99-105. https://doi.org/10.1109/SERA54885.2022.9806746
[41] Visoottiviseth, V., Kotarasu, C., Cheunprapanusorn, N., Chamornmarn, T. (2019). A mobile application for security assessment towards the internet of thing devices. In 2019 IEEE 6th Asian Conference on Defence Technology (ACDT), Bali, Indonesia, pp. 1-7. https://doi.org/10.1109/ACDT47198.2019.9072921
[42] Savolainen, T. (2023). A safe learning environment from the perspective of Laurea University of applied sciences safety, security and risk management students and staff. Heliyon, e12836. https://doi.org/10.1016/j.heliyon.2023.e12836
[43] Jensen, R.C., Bird, R.L., Nichols, B.W. (2022). Risk assessment matrices for workplace hazards: Design for usability. International Journal of Environmental Research and Public Health, 19(5): 2763. https://doi.org/10.1016/j.energy.2021.121907
[44] Sluser, B., Plavan, O., Teodosiu, C. (2022). Environmental impact and risk assessment. In Assessing Progress Towards Sustainability, pp. 189-217.
[45] Firera, R., Iskandar, A. (2022). Community service monitoring information system at the level of community harmony of citizens. Ceddi Journal of Information System and Technology, 1(1): 28-34. https://doi.org/10.56134/jst.v1i1.6
[46] Mustapa, M., Rahmah, U., Asjart, M. (2022). Development of learning media for introductory information and communication technology courses. Ceddi Journal of Education, 1(1): 23-27. https://doi.org/10.56134/cje.v1i1.11
[47] Iskandar, A. (2022). Developing a word composition educational game for young children after the Covid-19 pandemic. Ceddi Journal of Education, 1(2): 19-24. https://doi.org/10.56134/cje.v1i2.27
[48] Wirtz, B.W., Weyerer, J.C., Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. Government Information Quarterly, 39(4): 101685. https://doi.org/10.1016/j.giq.2022.101685
[49] Saeidi, P., Saeidi, S.P., Sofian, S., Saeidi, S.P., Nilashi, M., Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. Computers in Human Behavior, 63: 67-82. https://doi.org/10.1016/j.csi.2018.11.009
[50] Latvakoski, J., Öörni, R., Lusikka, T., Keränen, J. (2022). Evaluation of emerging technological opportunities for improving risk awareness and resilience of vulnerable people in disasters. International Journal of Disaster Risk Reduction, 80: 103173. https://doi.org/10.1016/j.ijdrr.2022.103173

APPENDIX

Charging instructions

The following checklist is a list consisting of several types of risks related to operational aspects of the iGracias SMK Telkom Makassar information system. You are expected to tick (√) the existing risks with the following conditions (Table A1):

(1) The check mark (√) in the YES option means that the risk is relevant to the existing risks in iGracias and the possibility of that risk occurring.

(2) The check mark (√) in the NO option means that the risk is not relevant to the risks that exist in iGracias and that risk is not possible to occur in the iGracias system.

Table A1. IGracias SMK Telkom Makassar

No	Risk Name	Description	Yes	No
1	Abuse of access rights	The risks that arise can result in changes to important data in the iGracias system		
2	Device theft	There will be financial losses in operations		
3	Limited access bandwidth	Resulting in the information system not being able to be accessed		
4	Feasibility of data input	Can result in invalid reports to leadership		
5	There is no regular maintenance	This will cause more serious damage to the device and result in losses		
6	Delay in helpdesk response	The helpdesk was negligent and not thorough (human error)		
7	Misunderstanding of user requests	Helpdesk is unresponsive in handling incidents		
8	Staff double duty	The risks that arise can give rise to other tasks in carrying out the duties and responsibilities as staff		
9	Server down	The risks that arise result in the iGracias information system being inaccessible		
10	Database error	The risk that occurs causes data not to be stored/input		
11	Human error	A procedural error causes damage		
		Security Threat Risk		
12	Hacking the network	Data damages the system by taking advantage of security gaps in a system.		
13	Attacked by malware	The impact on application/program data will be damaged or even lost		
14	Vulnerability	Risk of creating vulnerabilities/security flaws in the system		
15	SQL injection	If an attacker gets the administrator username and password from the database, it is possible for the attacker to take over an information system		
16	Cross-Site Scripting (XSS)	The risk that occurs can take over the user's account		
17	Ping flood	Stops data packets from unknown IPs		
18	Network failure	Data is not saved due to network damage		
19	Media failure	Data is not saved because the extension is not supported		
20	Disk failure	Hard disk bad sectors		
21	Snifing	One can see the data packet information such as username and password. Via a computer network		
22	DDOS	Attacks on servers that can cause the server to go down		
23	Data theft	Resulting in data loss on the system		
		Incidental risk		

24	Flood	The risk that will occur will result in asset damage
25	Lightning	The risk that will occur will result in asset damage
26	Earthquake	The risk that will occur will result in asset damage
27	Wind	The risk that will occur will result in asset damage
28	Fire	The risk that will occur will result in asset damage
29	Short circuit electricity	The risk that will occur will result in asset damage
30	DDOS	Attacks on servers that can cause the server to go down
31	Data theft	Resulting in data loss on the system

Probability and risk impact questionnaire

Based on the description above in the impact and probability table, it is expected to give a sign (√) to the probability and impact criteria (Table A2-A4):

Table A2. Process Risk

Risk Code	Types of process risks	Probability					Impact				
		1	2	3	4	5	1	2	3	4	5
R001	Abuse of access rights										
R002	Device theft										
R003	Limited access bandwidth										
R004	Failure to enter data										
R005	No hardware maintenance Periodically										
R006	Staff double duty										
R007	Server down										
R008	Database error										

Table A3. Process Security Risks

Risk Code	Types of system security risks	Probability					No				
		1	2	3	4	5	1	2	3	4	5
R009	Hacking the network										
R0010	Attacked by malware										
R0011	Vulnerability										
R0012	SQLL injection										
R0013	Cross-Site Scripting (XSS)										
	Amount										
	Percentage										

Table A4. Incidental Risk

Risk Code	Types of incidental risk	Probability					Impact				
		1	2	3	4	5	1	2	3	4	5
R0014	Flood										
R0015	Lightning										
R0016	Earthquake										
	Amount										