Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions

Rachel Ganesen[1], Asmidar Abu Bakar[2], Ramona Ramli[3], Fiza Abdul Rahim[4], Md Nabil Ahmad Zawawi[5]
College of Graduate Studies, Universiti Tenaga Nasional, Malaysia[1]
College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia[2, 3, 5]
Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia[4]
Institute of Informatics and Computing Energy, Universiti Tenaga Nasional, Malaysia[2, 3, 4, 5]

***Abstract*—Most universities rely heavily on Information Technology (IT) to process their information and support their vision and mission. This rapid advancement in internet technology leads to increased cyberattacks in Higher Education Institutions (HEIs). To secure their infrastructure from cyberattacks, they must implement the best cybersecurity risk management approach, which involves technological and education-based solutions, to safeguard their environment. However, the main challenges in existing cybersecurity risk management approaches are limited knowledge of how organizations can determine or minimize the significance of risks. As a result, this research seeks to advance understanding to establish a risk assessment model for universities to measure and evaluate the risk in HEIs. The proposed model is based on theoretical aspects that we organized as follows: First, we review the existing cybersecurity frameworks to identify the suitability and limitation of each model. Next, we review current works on cybersecurity risk assessment in HEIs to evaluate the proposed risk assessment approaches, scope and steps. Based on the information gathered, we developed a risk assessment model. Finally, we conclude the study with directions for future research. The result presented from this study may give an insig1ht for HEIs staff to analyze what is to be assessed, how to measure the severity of the risk, and determine the level of risk acceptance, improving their decision-making on risk management.**

***Keywords*—Cyber security; risk assessment; university**

I. Introduction

Higher education institutions (HEIs) are prime targets for cybercriminals because their networks hold sensitive personal information about students, including their academic and financial data. Several education organizations and institutions have been victims of cyberattacks [1]. Cybercriminals in Asia exploit flaws in IT systems that support schools and universities in carrying out various attacks. Even before the pandemic, a massive data breach that had reportedly hit a prominent Malaysian university resulted in the personal data of over one million people being leaked online [2].

During the COVID-19 pandemic, every industry faces significant change and ongoing challenges. Like many other industries, the higher education sector has been overturned by the COVID-19 pandemic. In place of classroom instruction, many students are learning virtually and remotely. While the shift to remote education may have helped the governments better contain the spread of COVID-19, it is also added a layer of cybersecurity risks that higher education institutions (HEIs) are forced to confront.

When the pandemic forced HEIs to use online platforms to conduct classes and evaluates students, it created a new entry point for cybercriminals to target due to the vulnerabilities in online platforms. These platforms include video chat programs like Zoom and Microsoft Teams and curriculum, technology, and services providers. According to Malwarebytes, the education sector is the top target for Trojan malware [3]. Kaspersky discovered 356,000 malicious files while investigating infected online textbooks, including 233,000 malware-infected essays and 123,000 malware-infected books [4]. A recent Kaspersky study showed that the number of users exposed to various threats using common online learning sites as a lure reached 270,171 in January 2021, up 60% from the first half of 2020 [5]. The rapid development of internet technologies and online platforms among students has led to increased cyberattacks in HEIs.

Since new and more advanced threats arise at an unprecedented pace, it is evident that HEIs are at risk of potentially disastrous security incidents if adequate security measures and workforce preparation initiatives are not implemented. Representatives from every campus department, such as administration, facilities, communications, and IT, must work together to analyze potential risks and create policies to address them [6]. To secure their infrastructure from cyberattacks, HEIs must implement the best cybersecurity risk assessment approach, which involves technological and education-based solutions, to safeguard their HEI environment.

Risk assessment provides organizations with an accurate evaluation of the risks to their assets. It can help them prioritize and develop a comprehensive strategy to reduce risks [7]. As highlighted by Panchal [8], many institutions have limited or no visibility of their IT risk exposure. Furthermore, available resources are not utilized effectively to manage the risks. The primary concerns in current risk assessment methodologies are how HEIs can estimate the significance of risks and develop resolution capabilities to deal with or minimize the risks. [9].

Therefore, this study aims to establish a cybersecurity risk assessment model for HEIs. The proposed model is based on theoretical aspects that we organized as follows: First, we review the existing cybersecurity frameworks to identify the suitability and limitation of each model. Next, we review current works on cybersecurity risk assessment in HEIs to evaluate the risk assessment approaches, risk metrics and steps proposed. We developed a risk assessment model combining ISO 27005 and NIST SP 800-30 framework based on the information gathered.

II. Review of Current Cybersecurity Risk Assessment Literature

A. Cybersecurity Risk Assessment Frameworks

Risk assessment is an important methodology for cybersecurity that employs techniques to assist organizations in dealing with uncertain events [10]. It is a tool for assessing factors that contributes to a failure or loss that hinders the success of a project or business. Various risk assessment models are available, some of which are qualitative while others are quantitative, with a common goal of estimating the overall risk value.

The Software Engineering Institute developed OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) at Carnegie Mellon University to help the U.S. Department of Defense (DoD) address its security risks and challenges [11]. OCTAVE has two variants: OCTAVE-S and OCTAVE Allegro [12]. OCTAVE-S has fewer processes, adhering to the overall OCTAVE philosophy and thus simplifying application for small businesses. OCTAVE Allegro is a later variant focused on protecting information-based critical assets. The OCTAVE framework is workshop-oriented, requiring knowledge from three levels: senior management, operational area management, and staff. Many risk assessment practitioners agree that the detail level and complexity of the OCTAVE assessment approach have made it hard to adopt on a wide scale [13].

Facilitated Risk Analysis Process (FRAP) is a method where information security provision is considered as part of the risk management process. The main objective of the Facilitated Risk Analysis Process (FRAP) was to develop an efficient and disciplined process to ensure that information-related risks to business operations are considered and documented [14]. Table I shows how each risk analysis procedure is separated into three distinct sessions.

However, this model requires expert communications and internal managers' participation to collect data, making the process more time-consuming. Besides that, this framework is designed to analyze business and not comply with security requirements.

Another prominent framework is ISO 27005, the international standard that guides information security risk management processes that are needed for the implementation of an effective information security management system (ISMS) [13]. The stages of risk assessment consist of context establishment, risk identification, risk analysis, risk evaluation, and risk management [15]. ISO 27005 provides good examples of a threat catalogue, vulnerabilities, and various computation and plotting techniques for rating risk. However, the limitation of this framework is that it focuses on objectives, guidance, and concept but does not provide any criteria, scoring, or decision matrices.

National Institute of Standards and Technology (NIST) published the latest version of the Cybersecurity Framework. This framework categorizes cybersecurity practices in five domains: Identify, Protect, Detect, Respond and Recover. As for the NIST method, the risk assessment process is refined into nine steps. Each step has a clear goal and all the possible approaches to accomplish the goal, which alleviates the bias brought by merely depending on participants' or security evaluator's knowledge [16].

Table II summarizes the differences between all four frameworks. Each framework has been categorized based on five criteria: phases, data collection method, approach and complexity. The OCTAVE framework phases focus more on assets while ISO 27000 and NIST focus on data security. The FRAP framework focuses more on business analysis than security assessment. The data collection method for OCTAVE and FRAP is largely dependent on the participants' knowledge which can be time-consuming. Meanwhile, NIST's and ISO 27005 framework data collection method is not limited to participants' knowledge but includes conclusions and discoveries mentioned in other related documentation.

In terms of approach, the OCTAVE framework is based on methodology and has an implementation guide. The FRAP framework is based on guidelines and participants' decisions. Meanwhile, ISO 27005 focuses on objectives, guidelines, and concepts and does not really provide criteria, scoring, or decision matrices. The NIST framework enumerates all the possible approaches to process the data and has a specific target to facilitate the procedure.

The complexity of each framework is defined by the time consumed to process and gather the data, and it can be categorized as high, medium and low. High complexity requires more participation in data collection and more time to process the data. Medium complexity is when it requires an average number of participants in data collection and an average time to process the data. In contrast, low complexity is when fewer people are required for data collection and less time is required to process the data. As a result, NIST SP 800-30 and ISO 27005 frameworks provide the most complete and scientific approach among all the methods.

TABLE I. RISK ANALYSIS PROCEDURE IN FRAP

FRAP Session	Description
PRE FRAP	It takes about an hour and involves the business manager, project lead and facilitator. The project outcome depends on five key components: scopes statement, visual mode, FRAP team, meeting mechanics and agreement on definitions.
FRAP SESSION	It takes between 7 and 15 hours to complete and includes 15 people in the organization. The second session is to access threats with the existing control place. It has three phases: risk analysis, safeguard implementation and security assessment.
POST FRAP	It takes about an hour with the same attendees. The deliverables for this meeting include a summary of threats and existing controls, as well as a final report.

TABLE II. COMPARISON OF FOUR CYBERSECURITY RISK ASSESSMENT FRAMEWORKS

Framework	Phases	Data Collection Method	Approach	Complexity
OCTAVE	1. Development of a profile of threats related to the asset 2. Identification of vulnerabilities 3. Development of security strategies and plans	Requires knowledge from all three levels: senior management, operational level and steps but does not imply third-party experts	Method based	High
ISO 27005	1. Context of risk establishment 2. Risk Identification 3. Risk Analysis 4. Risk Evaluation	Requires knowledge from internal managers	Guidelines	Low
FRAP	1. Pre frap meeting 2. FRAP session 3. Post FRAP process	Requires knowledge from internal managers and experts	Guidelines	Medium
NIST SP800-30	1. System characterization 2. Threat identification 3. Vulnerability identification 4. Control analysis 5. Likelihood determination 6. Impact analysis 7. Risk determination 8. Control recommendations 9. Results documentation	Non-government organizations	Guidelines	Medium

B. Related Works on Cybersecurity Risk Assessment in HEIs

Jufri et al. [17] conducted a risk assessment on the Academic Information System asset on OCTAVE Allegro and ISO framework. This research focuses on the Academic Information System in Langlangbuana University that functions to protect its critical assets. The process of risk assessment is conducted based on the OCTAVE framework. The implementation of security control is based on ISO 27002.

Similarly, Chanchala Joshi [18] has also proposed a quantitative information risk assessment model based on the OCTAVE framework for the university computing environment. The proposed model quantitatively measures security risks by identifying threats and information processes within university network configuration. The first phase focuses on knowing weak points. The next phase concentrates on understanding which areas have the highest risks. The last phase pivots with creating an actionable remediation plan over the university environment's unique factor and finally generate powerful reporting to track recursive risk measurement activities. The major drawbacks of OCTAVE are its complexity and that it does not allow organizations to quantitatively model risk. In order to improve the security organization system, some standard principles are required.

Meanwhile, Hom et al. [19] and Suroso et al. [20] proposed a risk assessment model to identify, analyze and manage the risk of academic information systems in higher education using the OCTAVE Allegro method. The risk assessment was conducted based on four stages, where first they establish drivers, profile assets, identify threats and mitigate risks. This approach differs from the OCTAVE approach because OCTAVE Allegro focuses on information assets within the context of how they are used, where they are stored, transported and processed, and how they are affected by the threat, vulnerability, and disruption as a result [8].

Sulistyowati et al. [21] proposed a model to reduce the risk of security breaches with the combination of the OCTAVE framework and ISO 27001. The risk assessment was conducted based on the OCTAVE framework, while the information security control and risk mitigation analysis is based on ISO 27001. The sustainability of the proposed improvement method is based on lost expectancy and return on investment. However, this model focuses solely on the security requirements of information assets and not on data security in HEIs.

Table III summarizes the evidence discussed in this section which highlights that most risk assessment work in HEIs based on OCTAVE, OCTAVE Allegro and risk management is based on the ISO framework. Besides that, the scope of those proposed risk assessment models focuses more on the security of assets in HEIs rather than data security. Therefore, our study aims to explore risk assessment based on the NIST SP 800-30 and ISO 27005 framework.

III. PROPOSED MODEL

The proposed model is based on ISO 27005 framework for context establishment and NSIT SP 800-30 framework for risk assessment process. Fig. 1 illustrates the proposed model for this study.

A. Context Establishment

In our study, the context establishment is based on ISO 27005 framework. This process establishes essential criteria for information security management. The context establishment explained the scope and restriction of risk that are adjusted based on the information security level to be achieved.

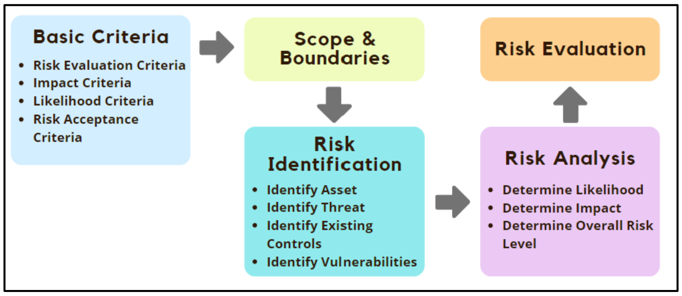

Fig. 1. Proposed Model.

TABLE III. RELATED WORKS ON CYBERSECURITY RISK ASSESSMENT IN HEIS

Authors	Objective	Scope	Framework	Phases
[17]	To assess the Academic Information System asset risk.	Academic Information System asset.	OCTAVE Allegro and ISO 27002	Risk assessment is conducted based on the OCTAVE framework. Implementation of security controls is based on ISO 27002.
[18]	To reduce the risks of a security breach.	Network configuration security	OCTAVE	Phase 1: Identification of weak points in university network configuration. Phase 2: Quantitative risk level measurement for the university's campus network. Phase 3: Enhancement of the university's security position.
[19]	To identify, analyze and manage the risk of academic information systems in HEI using the OCTAVE Allegro method.	Academic Information System	OCTAVE Allegro	Phase 1: Establish drivers Phase 2: Profile assets Phase 3: Identify threats Phase 4: Identify and mitigate risks
[20]	To identify the risk that affects the security of information assets and design some protection strategies for securing those risks.	Assets of Information System	OCTAVE Allegro	Phase 1: Establish drivers Phase 2: Profile assets Phase 3: Identify threats Phase 4: Identify and mitigate risks
[21]	The purpose of the proposed model is to reduce the risk of security breaches. The feasibility of the proposed improvement method is based on lost expectancy and return on investment.	Assets	OCTAVE and IS027001	Phase 1: • Understanding the information security needs. • Identify threats and vulnerabilities. Phase 2: • Identify likelihood. • Identify severity. • Risk assessment. Phase 3: • Analysis of Information security controls based on ISO 27000. • Calculation of loss expectancy. • Remediation plan.

1) *Basis Criteria*

a) Risk Evaluation Criteria: This study establishes the consideration in evaluating risk with these criteria:

- Confidentiality refers to the safeguarding of data against unauthorized access. NIST defined confidentiality as preserving authorized information access and disclosure restrictions, including safeguards for personal privacy and proprietary information [22]. In this study, when a hacker or other unauthorized individual gains access to a student information system, the students' data has lost its confidentiality.

- Integrity refers to the assurance that the data are unchanged from creation to reception. In this study, loss of integrity occurs when HEI data is accessed or modified by unauthorized parties, resulting in data accuracy and authenticity loss. For example, when a student's data is accessed or modified by a third party, the data's authenticity is not lost.

- Availability means the asset is always available to the authorized user [7]. In this study, loss of availability is defined as the state of an information system being unavailable, resulting in data loss and accuracy. The unavailability could be due to system disruption or malicious attacks by attackers.

b) Impact Criteria: The impact and likelihood of occurrence criteria are determined based on NIST SP 800-30 revision 1, where the rating scale is assessed from 5 being "Very High" to 1 being "Very low" and determined based on CIA triad of Confidentiality, Integrity and Availability. These criteria are presented in Table IV.

c) Likelihood Criteria: The likelihood of occurence criteria and likelihood of threat event resulting in adverse impact are adapted based on NIST SP 800-30 guidelines. Table V shows the likelihood of threat event resulting in adverse impact adapted based on NIST SP 800-30 guidelines. Table VI shows likelihood of threat event resulting in adverse impact.

d) Risk Acceptance Criteria: Risk acceptance is defined as the level of risk taking acceptable to achieve a specific business objective. Determining risk tolerance allows HEI to articulate how much risk the organization is willing to accept [23]. Table VII shows the risk tolerance appetite matrix based on NIST SP 800-30 guidelines.

TABLE IV. IMPACT RATING CRITERIA

Scale	Description	Value
Very High	Unauthorized disclosure of confidential data with a high number of records resulted in an adverse impact on HEIs. The unauthorized modification of the confidential data resulted in data damage or loss which cannot be recovered. The student system is not accessible for more than 24 hours.	5
High	Unauthorized disclosure of confidential data with a medium or low number of records seriously impacted HEIs. The unauthorized modification of the confidential data resulted in data being damaged/ missing, but data can be recovered. The student system is not accessible between 12 hours to 24 hours.	4
Moderate	Unauthorized disclosure of internal data resulted in a moderate impact on HEIs. The unauthorized modification of the internal data resulted in data being damaged/missing but can be recovered. The student system is not accessible between 2-12 hours	3
Low	Unauthorized disclosure of public data resulted in a low impact on HEIs. The unauthorized modification of the internal data resulted in data being damaged/missing but can be recovered. The student system is not accessible between 1-2 hours.	2
Very low	Unauthorized disclosure of unclassified data resulted in a low impact on HEIs. The unauthorized modification of the internal data resulted in data being damaged/missing but can be recovered. The student system is not accessible for less than 1 hour.	1

TABLE V. LIKELIHOOD CRITERIA

Scale	Frequency Number of a Possible Occurrence	Value
Very high	Between 20 to 30 times a year	5
High	Between 10-20 times a year	4
Moderate	Between 5 to 10 times a year	3
Low	Between 2 to 5 times a year	2
Very low	Less than 2 times a year	1

TABLE VI. RESULTING IMPACT SCALE

Scale	Impact Description	Value
Very High	Definitely give a negative impact	5
High	Almost certainly give a negative impact	4
Moderate	A medium probability gives a negative impact	3
Low	A small probability gives a negative impact	2
Very low	Very unlikely to have a negative impact	1

TABLE VII. RISK TOLERANCE MATRIX

Risk level	Impact Description	Scale
Low and Very Low	Risks are acceptable	1 - 4
Medium	Risks can be mitigated	5 - 15
High and Very High	Must be mitigated	15 - 25

2) Scope and boundaries: The scope of the risk assessment determines what will be considered in the assessment and what risk scenarios HEIs could anticipate. Risk assessment scope affects the range of information available to make risk-based decisions and is determined by the organizational official requesting the assessment and the risk management strategy. HEIs risk is not limited to information systems and security but includes financial, strategic, technological, and reputational risks [9]. In this study, our scope covers five types of risks as follows:

a) Strategic Risk: Strategic risk is related to corporate risk. It impacts the development and implementation of an organization's strategy. Strategic risk influence the organization's ability to achieve its long-term goals and objectives [13]. To effectively learn and adapt to new changes, top management needs to carefully define and implement a strategy. When a university implements a new strategy for its business process, the risk associated with that strategy should be considered. Since the COVID 19 pandemic, HEIs have shifted their teaching delivery from physical to online. If staff and students do not adapt to the new environment, the teaching procedures and academic achievement may deteriorate.

b) Operational Risk: The operational risk focuses on managing the risk that occurs in daily operations [9]. It is an occurrence that affects the organizations' ongoing management processes and procedures. Meanwhile, operational risk is defined by Panchal as the likelihood of human error or fraud in manual or automated environments. It also refers to potential threats to an institution's administrative process [11]. Inefficient or defective internal processes, people, control, system, or external events are the causes of business failures. For example, when a new learning management system is implemented in HEIs, teaching and learning activities are modified. If the changes are not effectively implemented, they may severely influence the ongoing student learning process, caused to system downtime and failure.

c) Compliance Risk: Compliance risk is concerned with the adherence to externally imposed laws and regulations, as well as internally bound policies and procedures concerning safety, conflicts of interest, and other issues. [20]. It is associated with conformance to federal, state, and regional rules and regulations [11]. It is concerned not only with externally imposed laws and regulations but also with internal policies and practices. This study investigates compliance risk in relation to research activities undertaken in an academic institution. The institution's research department must follow the laws and regulations of both the university and the government. Failure to comply with or violate applicable laws might result in severe penalties and accreditation revocation.

d) Financial Risk: Financial risk is associated with an initial assessment of HEIs revenues and expenditures and how to manage them [21]. Asset loss, conflict of interest, and technological risks are financial management or transaction events that harm an organization’s profitability and efficiencies. In this study, financial risk refers to the negative consequence of a cyberattack. Attackers can steal sensitive information, disable critical system access, and demand payment before restoring access. They have also threatened institutions with the publication or stolen critical information if they disagree with their requests. Some organizations must pay a ransom to regain access and recover lost data and systems. The sum paid may reduce the university’s budget or create insolvency, resulting in insufficient cash for other operations such as research, teaching, maintenance, and development.

e) Reputational Risk: Reputational risks are related to an organization’s brand or public image and emerge from the organization’s inability to handle any other type of risk accurately [20]. It also includes the external perception of the organization’s reputation. Reputational risk is frequently seen as a critical issue [13]. Political difficulties or unconstructive occurrences are examples of events that harm an institution’s reputation and public view. The impact of external perception on an institution’s image and brand is the focus of reputational risk [11]. This risk may occur due to an institution’s failure to manage any or all of the other risks effectively. HEIs must protect their valuable data, assets, and images from sustaining the university’s trust among students, parents, alumni, and the general public. Failure to successfully manage this risk will harm the university’s reputation, the inability to meet the target of student enrollment, and the failure to meet the target of business and research initiatives.

B. Risk Assessment

In this study, the risk assessment process will be based on NIST SP800-30 because the guidelines contain detailed criteria to analyze the risk.

1) Risk Identification

a) Identify Asset: Typically, a risk assessment encompasses all the organization’s critical assets that directly impact the confidentiality, integrity, and availability of the organization’s information resources [13]. Table VIII shows the example of information assets in the student information system.

b) Identify Threats: NIST [24] defined a threat as any circumstance or event that has the potential to negatively affect the organization, individuals, other organizations, or the nation’s operations and assets via an information system through unauthorized access, destruction, disclosure, or modification of information, and/or denial of service caused by threat sources. In this study, a threat is defined as a potential cause of an adverse event that may harm the HEI environment. Table IX shows an example of threat listings based on NIST SP-800 threat catalogues.

c) Identify Existing Control: The primary aim of this process is to consider both existing and proposed controls when determining the chance that a threat source would exploit the vulnerability. Hence, the more effective the control, the less likely a weakness would be exploited and vice versa.

d) Identify Vulnerabilities: This activity focused on identifying vulnerabilities that the identified threats could exploit. Examples of threat vulnerabilities scenarios are presented in Table X based on NIST SP 800-30 vulnerabilities catalogue.

TABLE VIII. EXAMPLE OF INFORMATION ASSETS IN THE STUDENT INFORMATION SYSTEM

Category	**Information Asset**
Student information system	Personal sensitive information. Student financial information. Student academic details. Student accommodation details. Study records of course completion and achievements.

TABLE IX. THREAT LISTING

Threat Agent	**Threat Action**
Students	Possible weak passwords due to lack of password complexity controls
Malicious insiders	System intrusion and unauthorized system access.
Hackers	Send phishing e-mails requesting students to enter their confidential details.

TABLE X. THREAT VULNERABILITIES SCENARIOS

Threat Agent	**Threat Action**	**Vulnerabilities**
Students	Open an e-mail requesting sensitive information or click on a malicious link that unknowingly downloads malware onto their device.	Lack of anti-virus and malware prevention.
Malicious insiders	System intrusion and unauthorized system access.	Weak password or due to lack of password complexity.
Hackers	Send phishing e-mails requesting students to enter their confidential details.	Insufficient security awareness and best practices.

2) Risk analysis: Risk analysis is about analyzing the elements that make up each risk scenario to determine [24]:

- The overall likelihood of a risk scenario occurring is calculated based on the combination of the likelihood that the event will occur and the likelihood that the event will have a negative impact.
- The impact (i.e., magnitude of harm) resulting from the occurrence of a risk scenario.

Table XI shows an assessment scale based on the NIST SP800-30 guideline to determine the overall likelihood.

The final risk rating is determined based on the intersection of the impact and overall likelihood for each identified threat and vulnerability pair. The formula to evaluate the risk is:

Risk = Overall Likelihood x Impact.

TABLE XI. OVERALL LIKELIHOOD

Likelihood of threat event initiation occur	**Likelihood of threat event results in adverse impact**				
	Very Low (1)	**Low (2)**	**Moderate (3)**	**High (4)**	**Very High (5)**
Very High (5)	Very Low	Moderate	High	Very High	Very High
High (4)	Very Low	Moderate	Moderate	High	Very High
Moderate (3)	Very Low	Low	Moderate	Moderate	High
Low (2)	Very Low	Low	Low	Moderate	Moderate
Very Low (1)	Very Low	Very Low	Very Low	Low	Low

Table XII depicts the risk appetite matrix used to determine risk. If the risk scores are in the black range, the risk is considered high. Meanwhile, if the risk falls into a grey shade, it is classified as moderate risk. If the risk is in the white shade, then the risk is categorized as low risk.

TABLE XII. RISK APPETITE MATRIX

Impact	**Overall likelihood**				
	1	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

3) Risk evaluation: Lastly, the derived risks will be evaluated according to the risk matrix score and compared to the risk tolerance level specified in the risk criteria. The output will take the next course of action to keep the risks within the organization's risk tolerance level.

IV. DISCUSSION

The core to effective university risk management is cybersecurity risk assessment. It is critical to select a suitable risk assessment approach that may give universities a range of instruments to identify unforeseen events and mitigate the impacts. We conducted extensive literature studies by evaluating existing risk assessment frameworks and related works on risk assessment in HEIs.

Based on our findings, we can conclude that the most dominant risk assessment literature in HEIs utilizes OCTAVE and OCTAVE Allegro framework for risk assessment and ISO 27005 framework for risk management. Hence, our study aims to explore ISO 27005 and NIST SP 800-30 frameworks to establish a risk assessment model for HEIs.

The context establishment and criteria are adapted based on ISO 27005 because it describes how to represent an incident process in risk scenarios. HEIs can assess the likelihood and impact that occurs in the scenarios of information risk to information security with the aid of incident description of risk scenarios. Meanwhile, the risk assessment process is based on the NIST SP 800-30 framework since it includes criteria, scoring, and decision matrices for analyzing risk, whereas ISO 27005 solely focuses on objectives, guidelines and concepts.

V. CONCLUSION AND FUTURE WORKS

This study aimed to establish a cybersecurity risk assessment model for HEIs by modeling the factors associated with HEIs. The method is based on the prominent ISO 27005 and NIST SP 800-30 frameworks. The primary goal of risk assessment in HEIs is to measure the risks and to improve their decision-making in managing the risk within the environment. A proposed cybersecurity risk assessment model was developed, demonstrating that several critical scenarios may arise in the HEIs environment. After evaluating the identified risks, the next step is to identify and determine the next course of action to keep the risks within the organization's risk tolerance level. Future research initiatives could further enhance the proposed model on establishing appropriate countermeasures for risk treatment in the HEI environment.

ACKNOWLEDGMENT

The Universiti Tenaga Nasional funds this research under the BOLD 2021 grant.

REFERENCES

[1] K12 Cyber Secure, "The K-12 Cybersecurity Resource Center The K-12 Cyber Incident Map," The K-12 Cyber Incident Map, 2021. https://k12cybersecure.com/map/ (accessed Mar. 27, 2021).

[2] A. Yeoh, Q. Tariq, and S. Menon, "UiTM students ' data allegedly stolen," The Star, 2019. https://www.thestar.com.my/news/nation/2019/01/26/uitm-students-data-allegedly-stolen-classified-records-compiled-over-18-years-believed-taken-from-va/.

[3] W. Zamora, "Trojans, ransomware dominate 2018–2019 education threat landscape," Malywarebytes Labs, 2019. https://blog.malwarebytes.com/trojans/2019/08/trojans-ransomware-dominate-2018-2019-education-threat-landscape/ (accessed Mar. 27, 2021).

[4] Kaspersky Team, "Student surprise : Malware masked as textbooks and essays Download an essay , get some malware thrown in Which types of malware are disguised as textbooks and essays ?," Karpersky Daily, 2019. https://www.kaspersky.com/blog/back-to-school-malware-2019/28316 / (accessed Mar. 27, 2021).

[5] S. Williams, "Cyber criminals target education sector as remote learning increases," Security Brief, 2021. https://securitybrief.eu/story/cyber-criminals-target-education-sector-as-remote-learning-increases (accessed Mar. 27, 2021).

[6] R. Sani, "Curbing cyber threats in online learning," New Straits Times Times, 2020. https://www.nst.com.my/education/2020/05/592083/curbing-cyber-threats-online-learning.

[7] A. S. Sendi, M. Jabbarifar, M. Shajari, and M. Dagenais, "FEMRA: Fuzzy expert model for risk assessment," 2010, doi: 10.1109/ICIMP.2010.15.

[8] P. Panchal, "Information Technology Risks in Higher Education: Strategy for Assessment, Planning and Management," CIO Review, 2022. https://education.cioreview.com/cioviewpoint/information-technology-risks-in-higher-education-strategy-for-assessment-planning-and-management-nid-4585-cid-27.html.

[9] S. S. Hassen and M. S. Zakaria, "Managing university IT risks in structured and organized environment," Res. J. Appl. Sci. Eng. Technol., vol. 6, no. 12, pp. 2270–2276, 2013, doi: 10.19026/rjaset.6.3858.

[10] D. Rios Insua, A. Couce-Vieira, J. A. Rubio, W. Pieters, K. Labunets, and D. G. Rasines, "An Adversarial Risk Analysis Framework for Cybersecurity," Risk Anal., vol. 41, no. 1, pp. 16–36, 2019, doi: 10.1111/risa.13331.

[11] C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson, “Operationally Critical Threat, Asset, and Vulnerability Evaluations (OCTAVE(SM)) Framework, Version 1.0. Carnegie Mellon Software Engineering Institute,” 1999. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473.

[12] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” 2007. [Online]. Available: https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf.

[13] M. Talabis and J. Martin, Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Syngress, 2013.

[14] T. R. Peltier, Facilitated Risk Analysis Process (FRAP). Auerbach Publications, 2001.

[15] A. Refsdal, B. Solhaug, and K. Stølen, “Cyber-Risk Management,” in Cyber-Risk Management. SpringerBriefs in Computer Science., Springer, 2015.

[16] N. A. Hashim, Z. Z. Abidin, N. A. Zakaria, R. Ahmad, and A. P. Puvanasvaran, “Risk assessment method for insider threats in cyber security: A review,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 11, pp. 126–130, 2018, doi: 10.14569/ijacsa.2018.091119.

[17] M. T. Jufri, M. Hendayun, and T. Suharto, “Risk-assessment based academic information System security policy using octave Allegro and ISO 27002,” Proc. 2nd Int. Conf. Informatics Comput. ICIC 2017, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/IAC.2017.8280541.

[18] C. Joshi and U. K. Singh, “Information security risks management framework – A step towards mitigating security risks in university network,” J. Inf. Secur. Appl., vol. 35, pp. 128–137, 2017, doi: 10.1016/j.jisa.2017.06.006.

[19] J. Hom, B. Anong, K. B. Rii, L. K. Choi, and K. Zelina, “The Octave Allegro Method in Risk Management Assessment of Educational Institutions,” Aptisi Trans. Technopreneursh., vol. 2, no. 2, pp. 167–179, 2020, doi: 10.34306/att.v2i2.103.

[20] J. S. Suroso and M. A. Fakhrozi, “Assessment of Information System Risk Management with Octave Allegro at Education Institution,” Procedia Comput. Sci., vol. 135, pp. 202–213, 2018, doi: 10.1016/j.procs.2018.08.167.

[21] I. Sulistyowati and R. V. H. Ginardi, “Information Security Risk Management with Octave Method and ISO/EIC 27001: 2013 (Case Study: Airlangga University),” IPTEK J. Proc. Ser., vol. 0, no. 1, pp. 32–38, 2019.

[22] NIST, “Guide for Conducting Risk Assessments,” 2012. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-30r1.

[23] ISACA, “ISACA, CRISC Review Manual 6th Edition,” 2015. CSA, “Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure,” no. December, 2019.