INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 12, Issue 4, (2022) E-ISSN: 2222-6990

Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions

Balla Moussa Dioubate, Wan Daud, Wan Norhayate

Faculty of Business and Management, Universiti Sultan Zainal Abidin

Corresponding Authors Email: ballamoussa1508@gmail.com

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v12-i4/12300 DOI:10.6007/IJARBSS/v12-i4/12300

Published Date: 12 April 2022

Abstract

Implementation of a cybersecurity risk management framework is one of the security management requirements in Malaysian public universities. It is critical to understand an institution's overall security profile. Therefore, this study aims to identify the current practice of cybersecurity risk management in Malaysian institutions of higher learning to address the security defies. This research employs a qualitative approach using a semi-structured interview to evaluate the current frameworks. This study considers the literature review on the cybersecurity risk management framework in Malaysian higher education institutions for data analysis. Thus, NVivo 12 software and thematic analysis were used to analyze the interview transcription from the audio recording. This paper expects to find the list of current frameworks applied in higher education institutions. It allows covering a wide range of cybersecurity risk management problems within the universities operation system. It is hoped that this study will make significant contributions to the cybersecurity risk management lifecycle in Malaysian institutions of higher learning.

Keywords: Cybersecurity Risk Management, Cybersecurity Risk Management Frameworks, Higher Education Institutions.

Introduction

Universities' development process suffers yearly because of a weak cybersecurity risk management plan (Grajek, 2020). According to Gordon (2015), many administrators of higher education institutions consider cyber security attacks as a tremendously critical problem confronted by their institutions. However, one of the main problems for colleges and universities is discovering a peer group enthusiastic about sharing high standards of cybersecurity risk management and losses suffered due to weak risk management. Loss or circulation of confidential information may provoke property damage, loss of pecuniary, and the university's reputation (Boranbayev et al., 2015). Thus, the threat to cybersecurity generated by the institution aggressive the ethical integrity of the organization's provision of services. However, it is believed that only technical resolutions are not adequate to solve

cybersecurity problems in higher education institutions as it does not adequately address the human aspect (Siponen, 2000; Spears & Barki, 2010).

There is a lack of cybersecurity risk management standards and best practices in higher education institutions. Consequently, organizations need appropriate cybersecurity risk management standards (ISO/IEC 27005:2018). There is still room for more strong enforcement of risk management policy and standards in higher education institutions (Kotulic & Clark, 2004). The increase of cybersecurity issues occurrences in academic environments shows the need to apply a recommended security management standard. On the other hand, one of the challenges for higher education institutions is to implement a cybersecurity policy effectively based on risk analysis by following the organization's requirements. It is revealed that, in case of security breaches or violations in universities, it is less likely to enforce regulations due to incomplete or incomprehensible security policies document (Ghazvini et al., 2018).

The existence of varied methods, principles, rules, and cybersecurity risk evaluation specifications has led the organization to face the frightening task of determining the most appropriate way to meet its needs. Therefore, there is a need to implement cybersecurity risk management standards as information security threats, national security rules, and specific business motives (Sari et al. 2016). However, cybersecurity risk management is one of the requirements of security management, and it is significantly essential in understanding the entire security profile of organizations. It is also crucial in information technology governance (Talet et al. 2014; Webb et al., 2014). Hence, recognize the significance of managing cybersecurity risk to higher education institutions. This study aims to discover more about cybersecurity risk management frameworks in Malaysia's higher education institutions. This paper will organize into the following sub-topics. Firstly, this paper will explain the introduction and the literature review. This is followed by the research method, results & discussions, and conclusion. Finally, this paper concludes with some limitations and suggestions for future study.

Literature Review

Cybersecurity

Clinch (2009) said that security is the dynamic safety of information, whether it is stored or carried. Besides, Nunes (2018) revealed that sensitive business information should be shielded from harm, and that's the purpose of cybersecurity with its three base pillars protecting confidentiality, integrity, and availability of information. Cybersecurity deals with information not being revealed to unauthorized individuals and is usually achieved by encryption. The integrity of information invalidates data tampering and destruction. Therefore, the complete information could be promptly obtainable to those with an authorized demand vital for company efficiency. Information security is not always considered in the design and development of information systems (Nunes, 2018).

Any unintentional or deliberate incident that could cause any harm to the computer system, causing content, financial or other losses to the organization, is considered to be a threat (Gómez, 2014). Cybersecurity is seen as a discipline that deals with tangible and intangible asset protection (Quintero et al., 2019). It allowed other characteristics to be included, such as authenticity, traceability (accountability), non-repudiation, and reliability (Escrivá et al.

2013). By considering the controls, it aims to ensure that security characteristics are functional (Peso & Ramos, 2015). In other words, by applying its principles, security measures can counter the threats to which the organization's digital assets are exposed to be embedded in computer systems, information, hardware, and software components. Cybersecurity requires the design and implementation, in very complicated ways, of a series of interrelated security measures (Álvarez & Pérez, 2004).

However, the cybersecurity risk management framework applied in higher education institutions can be handled technically and could be ineffective if not indorsed by an information security management system (ISO/IEC 2013). The accurate assessment of cybersecurity risks can be more complicated than assessing other types of risks because the data on the likelihood and costs associated with cybersecurity risks are usually limited, and the risks factor often keeps changing (Boltz, 1999). Cybersecurity's best-practice standards, such as the ISO/IEC (2013) series, suggest various managerial and technical controls to protect information resources. The standards admit that the level of security risks exposure must guide an organization's selection of rules. Therefore, organizations are advised to adopt a cybersecurity risk management approach (Webb et al., 2014; Talet et al., 2014).

Cybersecurity Risk Management

Cybersecurity risk management is the precondition of security management and is greatly meaningful in understanding the whole security profile of organizations. It is also one of the main functions of information technology governance (Talet et al., 2014; Webb et al., 2014). A successful information technology security requires an effective risk management process that provides an appropriate E-business atmosphere, as information technology systems are characterized by high degrees of risk (Boltz, 1999; Talet et al., 2014). The international standards ISO/IEC 27001 and ISO/IEC 27002 are involved in designing a cybersecurity management system by referring to cybersecurity risk assessment (Clinch, 2009).

Hashim & Razali (2019) postulated that the cyber security risk management process allows many enterprises to perform, in the most cost-efficient manner, a mitigate level of business risks. Therefore, an effective control strategy is to accept the risks and their assets without protection (safeguard) or control, prevent or avoid risks, apply rules to mitigate risks, or transfer risks to third parties. Besides, risk management practices are formulated to incorporate control (safeguard) or safety measures based on a risk assessment judgment. According to the standard ISO/IEC (2018), the cybersecurity risk management processes are illustrated: context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review.

Risk Context Establishment, this background of the study made by Nunes (2018), includes the concept of specific risk management principles. The external and internal context for cybersecurity risk management should be created, which defines the scope and bounds of cybersecurity risk management and develops an appropriate organization to operate the information security risk management. The company should limit cybersecurity risk management (ISO/IEC 27005).

Risk Assessment categorizes and measures the different types of risks to facilitate decision-making. Therefore, it requires information about assets and the exposed threats (Bojanc & Jerman-Blažič, 2012; PCI Security Standards Council, 2012). As a step of risk management, risk assessment is a mechanism that identifies assets and risks, including the anticipated frequency and potential for risk occurrence, by determining risk acceptance requirements, assessing risk levels, and defining impacts (Hashim & Razali, 2019). Risk assessment is a risk management step that defines suitable control methods for reducing or eliminating those risks. Therefore, it is categorized by the following three steps: risk identification, risk analysis, and risk evaluation. It shows a significant role in risk management in the organization, especially when there is a high dependency on information technology (ISO/IEC 27005; Wang & Liao, 2008).

Risk Treatment, according to ISO/IEC 27005:2018, cybersecurity risk treatment options are selected following the consequence of the risk assessment, the expected cost for applying these options, and the potential benefits from these options. A risk treatment design should be described that identifies the priority is arranged for that individual risk treatment. Preferences can be instituted employing various methods, encompassing risk ranking and cost-benefit analysis (ISO/IEC 27005). In consultation with the Risk Treatment Plan, this decision should be taken by the company's top management. Communication and consultation on cybersecurity are processes that should always be present to agree on effective communication between stakeholders on the risk management strategy (Nunes, 2018).

Risk Acceptance from one alternative from risk mitigation plans should specify how to evaluate risks to fulfill risk acceptance criteria. Responsible management must examine and approve proposed treatment programs and residual risks and document any conditions connected with such approval. Risk acceptance criteria can be more sophisticated than assessing if a residual risk is more than or less than a single onset. In certain situations, the degree of residual risk does not fulfill risk acceptance requirements because the criteria used do not take current conditions into account. Risk acceptance requirements are specifically associated with the goals and strategies of the company and take into account the needs of the stakeholders (ISO/IEC 27005:2018). However, rapid revision of the risk acceptability criteria is not always achievable. Decision-makers can accept risks that do not fulfill standard acceptance criteria in such situations. If this is required, the decision-maker should openly remark on the dangers and provide reasons for the choice to deviate from standard risk acceptance criteria (ISO/IEC 27005:2018).

Risk Communication Risk communication is an activity that involves decision-makers and other stakeholders discussing and sharing risk information to reach an agreement on how to manage risks. The report covers the existence, type, form, likelihood, severity, treatment, and acceptability of hazards, among other things. Effective communication among stakeholders is critical because it may significantly influence decision-making. Communication ensures that individuals in charge of risk management and others with a vested interest understand the reason for decisions and why certain measures are necessary (ISO/IEC 27005:2018).

Risk Monitoring and Review, ongoing monitoring, and evaluation are required to ensure that the context, the conclusion of the risk assessment and treatment, and management strategies remain relevant and suitable to the conditions. The organization should ensure that the cybersecurity risk management methodology and related activities remain ideal in the current conditions and are followed (ISO/IEC 27005). Furthermore, the organization should regularly confirm that the criteria used to assess risk and its components are relevant and aligned with corporate objectives, plans, and policies. It should also ensure that changes in the business context are regularly taken into account during the cybersecurity risk management process (ISO/IEC 27005).

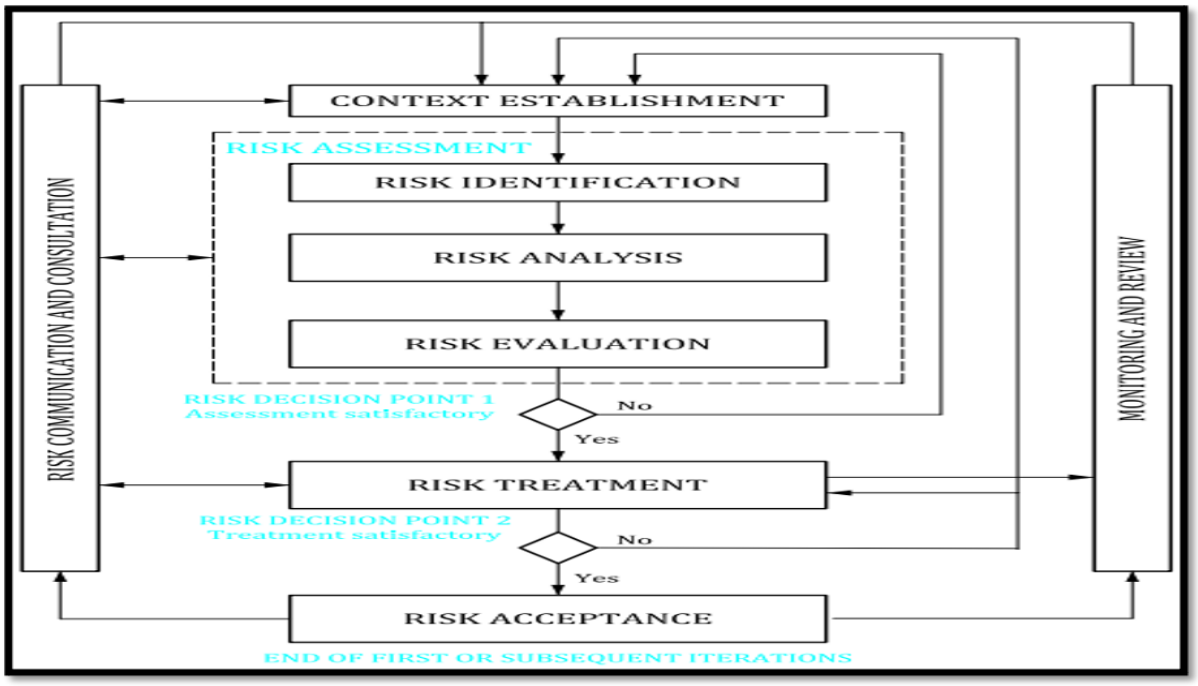

Figure 1: Illustration of an information security risk management process
Source: ISO/IEC 27005:2018

Research Methodology

The qualitative research method is employed to complete the studies concerning different areas, including preferences, in plain and customary terms (Yin, 2011). According to Creswell (2009), qualitative research examines and interprets the significance that individuals or groups are assigned to a social or human issue. The study method includes emerging problems and techniques, data usually collected in the participant's environment, inductively developing data interpretation from data to general themes, and the researcher interpreting the significance of the data. The final written report is organized versatilely (Creswell, 2009). This study considered the qualitative holistic multiple case study design due to the need for the researcher's get responses from professionals in cybersecurity risk management regarding the current method used in higher educational institutions. The holistic multiple case study approach was the main fitting research design since this study investigated strategies utilized to manage the risks related to cybersecurity in Malaysian public universities. This study aimed to identify the current cybersecurity risk management frameworks in Malaysian public universities. This study included a multiple-case design of 10 cases of public universities in Malaysia.

The population is essential for solving the research problems because higher education intuitions have greater compliance with cybersecurity policy (Feehan, 2013). Therefore, the population for this research was mainly the twenty (20) public universities in Malaysia. The sampling of 10 public universities and 12 cybersecurity risk management officers from the departments in charge of cybersecurity risk management contributed to this study. The data provided were enough to reach data saturation. Thus, the researchers drew the sample frame of this study from 10 accredited public universities in Malaysia. The researcher collected information until no new information was accessible to attain data saturation. which means the repetition of data started, and no further information was available. Therefore, no new themes emerged after interviews with 12 participants from 10 public universities in Malaysia. Interviews found the primary data source, whereas the secondary data source includes observations and records. The research design, data collection technique, and implementation of data collection methods were appropriate to answer the research question (Okoye, 2017). In this study, the researchers interviewed experts (cybersecurity risk management) to receive feedback on their current cybersecurity risk management methods. The researchers recorded the interviews with participants from the department in charge of cybersecurity risk management in Malaysian higher education institutions and transcribed word–to–words. Each participant involved in the interview was categorized by a portion of the speech associated with the code number of each participant. The Pseudonyms P (1) to P (10) represented the 10 participants accordingly) to locate each portion of the interview transcript.

Moreover, advanced coding utilizing the NVivo 12 computer program is valuable. Therefore, Houghton et al (2013) famous that the NVivo 12 computer program is advantageous as data management that can give a comprehensive audit trail to delineate decisions made within the research procedure. Thomas (2015) used auto-coding in the NVivo 12 computer program to code qualitative data. The researcher used NVivo 12 software for coding based on the transcripts made from the interview record, documents, and observations to identify the words used by respondents during the interview. The researcher applied the auto coding method to categorize data based on research questions.

Findings

The investigation results come from 12 participants who experienced in-depth, face-to-face interviews, which were conducted with cybersecurity risk management officers from 10 public universities in Malaysia. This section highlights the interview findings from the ten universities samples presented in Table 1. The two themes answered the research question: What cybersecurity risk management frameworks are used in Malaysian higher education institutions?

Table 1 Research Question, Themes, Sub-Themes, Sources, and References exported from NVivo 12 software.

Research Question	Themes	Sub-Themes	Sources	References
What are the cybersecurity risk management frameworks used in Malaysian higher education institutions?	Risk Management Frameworks	Frameworks Implementation Issues	3	10
		Identification and Implementation	4	11
		Types of Frameworks	8	37
	Risk Management In Education Institutions	Management	9	24
		Risk Management	5	13

Risk Management Frameworks

The theme Risk Management Approaches discussed the different frameworks and models currently used in the public universities of Malaysia and those in the implementation process. The theme allowed us to know about the identification and implementation issues of practicable cybersecurity risk management frameworks in public higher education institutions. The theme, risk management Frameworks, included the following subthemes: Type of Frameworks, Frameworks Identification, and Implementation, and Framework Implementation Issues.

Type of Frameworks

Public Universities in Malaysia are using different frameworks by following the real environment of the institution as mentioned by the following participants:

"We started by using something called Hazard Identification and Risk Assessment Framework (HIRA).. and also we have used the framework of The Malaysian Public Sector Cybersecurity Risk Assessment System (MYRAM) … But later this university has started to look at The Information Security Management System (ISMS)" and also ISO 27000 related (ISO 27001:2013) to Information Security Management..."

"We have 2 frameworks in place now one is ISO9000, It's a quality management system. Because we implemented the Quality Management System (QMS), specifically for data security we have another one that we call Information Security Management System (ISMS). … and ISO 27000 the certification framework to judge our security management …."

"We have 3 main documents frameworks; these frameworks are … ISO 9001:2015 that framework combined with ISO 27001:2013 so these two frameworks combined to become the university risk management framework … Also, another document we refer to is enterprise risk management briefly two frameworks basically, the enterprise risk management is just additional."

"Ok, currently we are using… ISO27001:2013 this one is the information security risk management system..."

"We used a framework that had been introduced by SIRIM known as IEC/ISO27001:2013 Information Security Management System (ISMS)."

"We are using the ISMS and information security management system ISO 27001: 2015… We have ISO 27001: 2015 …for financial and Australian standard template use to manage the risks including the cybersecurity risk".

"I think even though in many places there is no specific one. We use a certain component in the framework from a different framework because some might be suitable some might not be suitable."

According to the above statements from the participants, the researchers can conclude that the main framework utilized by most of the participants was the ISO 27001: 2013 international standard used as a specification for ISMS. However, some universities have migrated from one framework to another, whereas others have combined different frameworks to develop the current framework. The List of additional frameworks used by Malaysian public universities is MYRAM, HIRA, ISO 27000 related to Information Security Management, ISO9000 (QMS), ISO9001:2015, Enterprise risk management framework, ISO 27001: 2015 for financial and (SIRIM).

Identification and Implementation

The identification and implementation of the framework follow the policies and principles stated by the Malaysian government through the Malaysian Administrative Modernization and Management planning unit (MAMPU).

"We have been asked by the government especially the Ministry of Higher Education and also directives from "MAMPU" the Malaysian Administrative Modernization and Management Planning Unit ..., they have asked universities to start using "ISMS" … know the framework for implementation."

"One of the latest requirements of the "ISMS" is that the information security risk must be process basis rather than scoping it into related assets to IT. but it's supposed to support a complete process."

"MAMPU, it's not enforced. They just suggested doing it to enforce us to do the ISO 27001 once we are doing that one. So we have to identify and we have to follow the auditor from certifying body that certifies body will be SIRIM and Cyber Security Malaysia."

"*It is a dilation from the government… Every government university must use ISMS it is mainly used for security management, for risk management on IT on data security … So that's mean we are not choosing it is a direction from the government."*

The Malaysian Government instructed the implementation of risk management frameworks through the Malaysian Administrative Modernization and Management planning unit (MAMPU). The Government required the public university to implement Information Security Management System frameworks (ISMS), with the ISO 27001:2013 as support.

Frameworks Implementation Issues

The process of framework implementation instructed by the Malaysian Government faced some issues while applying. These are the university environment, the understanding of the guidelines, and the management structure of the institutions.

"I think to implement we need to give awareness to the staff which is quite difficult even the fact that we are not sure clear on how the because you need to know that ISMS they are categorizing the risk using the asset which is four categories…The process is really difficult because we need to identify… That was I think that was the difficult and challenges in part of that my face it the awareness is really difficult …. The challenges we encounter were the negative perception towards risk and what kind of awareness we should implement in educating."

"Ok, the first thing is to understand all the documents under ISO 27001, ok you to understand I think that is a challenge because we are from technical so we have to understand what it means for each of the annexes there 114 annex … and also how to measure I think our challenges now is how to measure the control."

"All these ISO is only a guideline and this guideline sometimes is only general so in terms of practicality you know that's why you need to try to adapt and try to look from a realistic perspective…, you must understand all the terms guidelines..."

"They may be familiar with the quality management standard which is you know ISO 9000 for example. But when it comes to information security standards ISO27000 or "ISMS". This is going to be new for them… and for many of them, this idea plus time dealing with this kind of new requirement so they had to learn."

"So because of budget we cannot do all of we cannot say all universities, we cannot say all the ICT services security protection is under ISMS no. We don't have enough money, manpower everything to do that"

"We need money, for example, we need a new type of server to Install a new technology that can strengthen the infrastructure of the security."

"I mean the main issue is cost. And you know the public university all rely on the government's funding. We are not like a private university. … So we need the allocations from the governments."

The framework's implementation issues mainly focus on lack of training and awareness, understanding of standards, and misunderstanding of the list policies. It is followed by the limitation of the budget for government universities to finance innovative projects in the institutions.

Risk Management in Education Institutions

The theme of risk management highlighted the core process involved in monitoring cybersecurity risk in Malaysian Public Universities. The theme discussed risk management

steps from people, processes, and technology. The sub-themes of Management and risk management were discussed.

Management

The Management planned the creation of a risk management team and the appointment of risk managers to each department. The internal and external audit was scheduled for the framework control and evaluation.

"The management of the framework covered other aspects including ICT, information system, security, and also other things especially for our operation our planning of our safety risk so that is the framework that we used."

"We have a management review meeting … Basically on the people and the financial part. you can see a commitment… convincing the management, management influences. The management interference regarding the simulation to make sure the process is up and running."

"Okay. The macro management for the framework started with the risk treatment plan. Okay, we must implement a risk treatment plan. … they have what we call management meetings. So we must report to the management meeting to the top-level vice-chancellor to our CEO."

"We give knowledge to all the known university people, staffs, of course, we have appointed risk managers for each department indicating they are the one that will be responsible to identify the risk ablated to their departments at our office."

"Our risk management team also has our risk management team from our technical staff this is from where they understand the system, the server stores the network so we have a set of a team, a team of risk management."

"The department invites us to give them a thought, we give them a thought face to face which is we think that was the most effective and then we do the face to face and at the first time we also appoint risk officer at all PTG."

Participants highlight the importance of having management support and teams. This explained how the risk management staff is organized in each faculty, managers were assigned to control, and a quarterly meeting was arranged. The participants talked about the necessity to have support from the management. This makes easy the adoption of a new framework in the university risk management system.

Risk Management

The general management of the framework is the crossways of the technology. It covers different aspects such as information and communication technology (ICT), information systems, operation planning, management team, and security.

"So from the data center management, we analyze what's the current situation risk for our data center… So in the end, the result is you know your risk levels with the three parameters; Low, Medium, and High.… Which part we are medium, which part we are low."

"I consolidate all the risk reports read, register and we bring to this board to discuss to endorse or to make decisions … you can look from one quantitative perspective sometimes you can look from the qualitative perspective how you measure risk."

"The risk was categorized: Definitely it is something very positive. Because we have categorized the risk according to some categories. We have the financial aspects, operation risk management aspects and then we have the government aspects, that government aspect."

"By identifying that we are going to categorize and then we are going to determine whether the asset has a high risk or low risk."

"Different system admin different has different perspectives of the risk …level office... The level of risk depends on the level of understanding."

"We are a novice… To be a success on the journey we need to have support from management that one should be number one because we already first thing first we need to get a blessing from management and once they bless then only you can move."

The management influenced the execution of the risk management process from risk identification to risk treatment. Participants identified the different types of risk strategic, human, compliance, and operation risks. The participants talked about the other risk management teams in the university. The particularity is the risk management team was built by the technical staff of the university.

Discussion

Risk Management Frameworks

The majority of the respondents from the study mentioned that the Malaysian government is generalized and recommended the framework implementation to plan and insert ISMS in all public universities in Malaysia. However, according to Shamala et al. (2015), the risk mitigation model involves the risk mitigation mechanism and the risk decision process informed by the technological and organizational risk elements and metrics. Information mapping and software agents also assist the system in helping practitioners make risk decisions. Joshi & Singh (2017) proposed a structure for universities and higher education institutions with a multi-disciplinary community. It is based on the most common OCTAVE risk system, the model-based risk assessment methodology (Joshi & Singh, 2017).

Innovation is critical for businesses, and economists, researchers, and practitioners have universally agreed that 'innovation is power' (Lind et al., 2018; Ibrahim et al., 2020). Therefore, organizations adopting the ISRM system or standards should consider the organizational structure and make appropriate adjustments as they wish to incorporate additional frameworks (Özçakmak, 2019). However, according to the participants in this study, an essential list of cybersecurity risk management frameworks was used in Malaysian public universities, which are: Security Risk Assessment System (MYRAM), Hazard Identification and Risk Assessment Framework (HIRA), ISO 27000 related to Information Security Management, ISO 9000 related to the quality management system (QMS), ISO 9001:2015, Enterprise risk management framework, ISO 27001: 2015 for financial, Australian

standard template for risk management, and Standard and Industrial Research Institute of Malaysia (SIRIM). Moreover, some universities have frameworks related to the data center to identify and treat risks associated with the data center.

However, the public universities mainly depended on the government. Therefore, there was a demand from the authority to implement cybersecurity risk management in public universities for security purposes. The implementation of risk management in educational institutions is hindered because they do not have the required organizational and administrative regulations and documents, complicating the analysis and control of risks (Suray et al. 2019). The head of the organization must prepare all the documentation required to ensure the report's development and guideline is structured. The vital regulatory documents for the risk control of the educational institution should include (Suray et al. 2019; Najwa et al. 2019). On the contrary, this study showed the positivity of implementing Information Security Management Systems (ISMS) by following the government recommendation to implement cybersecurity risk management frameworks and standards (ISO 27001: 2013).

Based on the review of participants and literature, it can be summarized that the public universities in Malaysia are using different types of frameworks based on the need and environment of the institutions. Some universities are using both standard ISO 27000 series, especially the version ISO 27001, and other frameworks created based on the university's environment. However, the ISO/IEC 27001-based Information Security Management System (ISMS) preparation mandates the responsible handling of risks directed at the confidentiality, integrity, and availability of information or other critical assets.

Risk Management and Education Institutions

The participant also said that the implication of management influenced the execution of the risk management process to facilitate the whole procedure, from risk identification to risk treatment. However, risk management processes require continuous improvement in managerial competencies. That is why the risk reduction management system should be a constant phase of development for administrative qualifications combined with diagnostics and forecasting, which eventually minimizes management risks and dramatically improves the efficacy of management activities (Suray et al., 2019). Top management trust in the technical staff would also improve due to using resources only to mitigate the real risks (Ozcakmak, 2019).

However, a previous study from Hommel et al (2015) indicated that its security governance had not been wholly accepted. several large companies have not had CISOS before their IT security breaches. also, the organizational frameworks that promote IT security management are still very complex, as shown by the various reporting structures, despite the evidence of the strategic role of IT security in creating business value. In publicly traded companies, the board is responsible and accountable to the shareholders and must ensure that the company generates business value for the stakeholders. thus, the CEO appoints an official, CISO, to oversee IT security management via direct reporting/communication (Hommel et al., 2015).
In general, the feedback from this research displayed the management procedure in the universities, the management influence, the process of risk treatment, the internal and external audit, the organization of the risk management team, and the appointment of risk

managers to each department. The management could plan to create a strong risk management team in the structure and the position of the risk managers in each department. However, some universities started the risk management comity, gave staff a permanent training session, and appointed the risk management officer. The senior manager can more explicitly communicate risk control and reporting processes to senior management. It is crucial to develop this value that will contribute significantly to IT security's effective and efficient management. As such, it is in the best interest of the management staff, especially the CEO, as an agent of the Board and stakeholders to ensure that IT resources are protected because of IT security.

Based on MS ISO 31000:2010, the risk management process includes contextualization, risk assessment, monitoring and analysis, and contact and consultation. Three practices are included in the risk evaluation, namely risk recognition, risk analysis, and risk assessment. Many of these risk management mechanisms are addressed in the following section (Shoki et al., 2014). Effective risk management is good governance. However, the participants talked about identifying the top risk from the university as a pre-preliminary condition, the misunderstanding of the risk, the risk identification, and categorization. The different stages involved in the analysis are from risk identification to risk treatment: the evaluation and the implementation of the primary recommended risk management method ISMS by the government.

Conclusion

This study revealed that the Malaysian Government directed the implementation of risk management frameworks through the Malaysian Administrative Modernization and Management Planning Unit (MAMPU). Most public universities used the ISO 27001: 2013 international standard as a specification for ISMS. Some additional frameworks were used, such as MYRAM, HIRA, ISO 27000 related to Information Security Management, ISO9000 (QMS), ISO9001:2015, Enterprise risk management framework, ISO 27001: 2015, and (SIRIM). However, there are framework implementation issues which include a lack of training and awareness, a lack of understanding of standards, and a misunderstanding of the list policies. The research further discovers that the management influenced the execution of the risk management process from risk identification to risk treatment in educational institutions. The formation of a risk management team and the assignment of risk managers to each department were planned by management. Management intended an internal and external audit for framework control and evaluation.

The higher education institutions should encourage implementing an adapted framework based on the university's environment to increase efficiency in areas such as risk evaluation, risk management, decision-making, and reporting that assist the organization in achieving its strategic goals and increasing institutional efficiency. Both participants agreed that written policies and a cybersecurity risk management framework across university systems are critical. The study's future aim will be to examine the impact of the cybersecurity risk management frameworks on the business performance of the higher education institutions in Malaysia. It will also propose updating cybersecurity risk management processes in the university's entire management cycles that the management can use in the university environment. The difficulties ahead are establishing risk management processes,

frameworks, or methodologies that are understandable and cost less to respond to university governance.

References

Alvarez, G., and Perez, P. (2004). Seguridad informática para empresas y particulares (Madrid: McGraw-Hill).

Bojanc, R. (2012). A quantitative model for information security risk management (pp. 267–275).

Boltz, J. (1999). Informational Security Risk Assessment: Practices of Leading Organizations. DIANE Publishing.

Boranbayev, A., Mazhitov, M., & Kakhanov, Z. (2015). Implementation of Security Systems for Prevention of Loss of Information at Organizations of Higher Education. *2015 12th International Conference on Information Technology - New Generations*, (It), 802–804.

Clinch, J. (2009). ITIL V3 and Information Security. Best Management Practice.

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approach. Thousand Oaks, CA: SAGE Publications.

Escrivá, G., Romero, R., Ramada, D., and Onrubia, R. (2013). Seguridad informática (Madrid: Macmillan Iberia S.A.).

Feehan. P (2013). Higher Education IT Compliance through the Prism of Risk Controls | EDUCAUSE.

Ghazvini, A., Shukur, Z., & Hood, Z. (2018). Review of information security policy based on content coverage and online presentation in higher education. International Journal of Advanced Computer Science and Applications, 9(8), 410–423. https://doi.org/10.14569/ijacsa.2018.090853.

Gómez, A. (2014). Seguridad en equipos informáticos (Madrid: Editorial RA-MA).

Gordon, C. J. (2015). Addressing Security Risks for Mobile Devices: What Higher Education Leaders Should Know.

Grajek, S. (2020). TOP 10 IT ISSUES 2020: The Drive to Digital Transformation Begins. *EDUCAUSE Review*, 4.

Hashim, R., & Razali, R. (2019). Contributing Factors for Successful Information Security Management Implementation: A Conceptual Model. International Journal of Innovative Technology and Exploring Engineering, 9(2), 4491–4499. https://doi.org/10.35940/ijitee.b7214.129219.

Hommel, W., Metzger, S., & Steinke, M. (2015). Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization.

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case study research. Nurse Researcher, 20(4), 12-17.

Ibrahim, H. I., Mohamad, W. M. W., & Shah, K. A. M. (2020). Investigating Information and Communication Technology (ICT) usage, knowledge sharing, and innovative behavior among engineers in electrical and electronic MNCs in Malaysia. Jurnal Pengurusan, 58, 133–143. https://doi.org/10.17576/pengurusan-2020-58-11

ISO/IEC. (2013). Information technology - Security techniques - Code of practice for information security controls, ISO/IEC 27002:2013(E).

ISO/IEC. (2018). Information technology — Security techniques — Information security risk management, ISO/IEC 27005:2018 (E).

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step

towards mitigating security risks in the university network. Journal of Information Security and Applications, 35(October 2018), 128–137. https://doi.org/10.1016/j.jisa.2017.06.006.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information and Management, 41(5), 597–607.

Leseure, M. J., Bauer, J., Birdi, K., Neely, A., & Denyer, D. (2004). Adoption of promising practices: A systematic review of the evidence. International Journal of Management Reviews, 5/6(3/4), 169–190. doi:10.1111/j.1460-8545.2004.00102.

Lind, C. H., Kang, O., Ljung, A., & Forsgren, M. (2018). MNC involvement in social innovations: The

issue of knowledge, networks, and power. Critical Perspectives on International Business 16(1): 79-99.

Najwa, N. A., Ramly, Z., & Haron, R. (2019). Board Size, Chief Risk Officer, and Risk-taking in Islamic Banks: Role of Shariah Supervisory Board. Jurnal Pengurusan, 57. https://doi.org/10.17576/pengurusan-2019-57-01

Nunes, S. R. (2018). Value-focused assessment of cyber risks to gain benefits from security investments.

Okoye, S. (2017). Strategies to Minimize the Effects of Information Security Threats on Business.

Özçakmak, F. (2019). Supplementing Isrm Models By Kri Implementation. Nanotechnology, 27(9). http://dx.doi.org/10.1016/j.cej.2014.10.020%0Ahttp://dx.doi.org/10.1016/j.apcatb.2013.08.019%0Ahtt p://dx.doi.org/10.1016/j.tsf.2016.12.015

PCI Security Standards Council. (2012). Information Supplement: PCI DSS risk assessment guidelines.

Peso, E., and Ramos, M. (2015). La seguridad de los datos de carácter personal (Madrid: Ediciones Díaz de Santos).

Quintero, N. A., Pérez, T. V., & Silva, H. C. (2019, June). Information security model. Case study higher education institution. In Journal of Physics: Conference Series (Vol. 1257, No. 1, p. 012014). IOP Publishing.

Shamala, P., Ahmad, R., Zolait, A. H., & bin Sahib, S. (2015). Collective information structure model for Information Security Risk Assessment (ISRA). Journal of Systems and Information Technology, 17(2), 193–219. https://doi.org/10.1108/JSIT-02-2015-0013.

Shoki, M., Zakuan, N., Tajudin, M. N. M., Ahmad, A., Ishak, N., & Ismail, K. (2014). A framework for risk management practices and organizational performance in higher education. Review of Integrative Business and Economics Research, 3(2), 422–432.

Siponen, M. T. (2000), "Critical analysis of different approaches to minimizing user-related faults in an information systems security: implications for research and practice", Information Management & Computer Security, Vol. 8 No. 5, pp. 197-209.

Spears, J. L., and Barki, H. (2010), "User participation in information systems security risk management", MIS Quarterly, pp. 503-522.

Suray, N., Karpenko, E., Dubovik, M., Shlyenov, Y., & Sterlikov, F. (2019). Risk Management At Educational Institution* Natal. 7(2), 1171–1184.

Talet, A. N., Mat-Zin, R., & Houari, M. (2014). Risk management and information technology projects. International Journal of Digital Information and Wireless Communications (IJDIWC), 4(1), 1–9.

Thomas, S. J. (2015). Exploring strategies for retaining information technology professionals: A case study (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3681815).

Wang, Y., & Liao Y. (2008). Understanding individual adoption of mobile booking service: An empirical investigation. CyberPsychology & Behavior, 11(5): 603-605. doi:10.1089/cpb.2007.0203.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*, 1–15.

YIN, R. K. (2011). Qualitative Research from Start to Finish. Animal Genetics (Vol. 39).