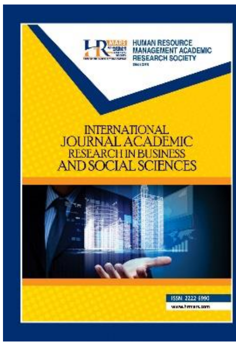
INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

MARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990



A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions

Balla Moussa Dioubate & Wan Daud, Wan Norhayate

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v12-i5/12924 DOI:10.6007/IJARBSS/v12-i5/12924

Received: *17* March 2022*, **Revised:** 19* April 2022*, **Accepted:** 30* April 2022

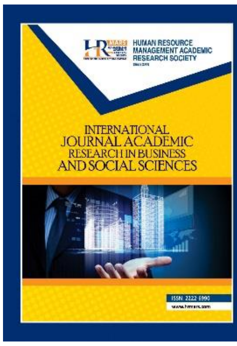
Published Online: 10 May 2022

In-Text Citation: (Dioubate & Wan Daud, 2022)

To Cite this Article: Dioubate, B. M., & Wan Daud, W. N. (2022). A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(5), 1081 – 1093.

Vol. 12, No. 5, 2022, Pg. 1031 – 1093

http://hrmars.com/index.php/pages/detail/IJARBSS **JOURNAL HOMEPAGE**



INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

HR MARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions

Balla Moussa Dioubate & Wan Daud, Wan Norhayate
Faculty of Business and Management, Universiti Sultan Zainal Abidin
Corresponding Author's Email: ballamoussa1508@gmail.com

Abstract

Cybersecurity risk management has been applied to many aspects of modern life, including banking, finance, health, life, business ventures, and project management. It is currently gaining much attention in universities for operation safety reasons. Higher education institutions have to face new challenges and increasing information technology threats more sophisticatedly. Therefore, this study will investigate the current cybersecurity risk management frameworks used in Malaysian public universities. The qualitative research method will be applied to collect data by interviewing experts in cybersecurity risk management. The literature review showed the primary constructs of the cybersecurity risk management framework for Malaysian universities. Moreover, the results show the factors that lead to risks and benefits obtained when the stakes are managed. The researchers will clarify the method or mechanisms for risk management in a university environment. This research shows a greater understanding and knowledge of risk management. The future direction of this study is to propose a cybersecurity risk management framework based on the reviews of the existing frameworks used in Malaysian public universities.

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

Introduction

The development of sophisticated devices poses a new security risk nowadays in higher education. According to Gordon (2015), many administrators of higher education institutions consider that security is tremendously a critical problem confronted by their institutions. However, risk management in cybersecurity is a requirement of security management, and it is significantly essential in understanding the entire security profile of organizations. It also plays a vital role in information technology governance (Talet et al., 2014; Webb et al., 2014). Therefore, a security risk management process allows many higher education institutions to accomplish a moderate level of risks in the most cost-effective way.

Though, in most Malaysian higher education institutions (HEIs), ethical hacking is not consolidated into their Security development life cycles (SecSDLC) (Kang et al., 2015). The authors noted that hackers are endowed with powerful tools with the rapid advancement of information technology. As a result, safeguarding information security is becoming a difficult task. Using hacking tools and methods, also known as penetration testing or ethical hacking, can help to reduce security risks. Managers, however, declined to assign this arm to protect their information from opposing hackers due to a lack of penetration assessment information. As a result, the number of victims of hackers in Malaysian higher education institutions continues to rise significantly (Kang et al., 2015).

Loss or circulation of confidential information may provoke property damage, loss of pecuniary, and the university's reputation loss (Boranbayev et al., 2015). Thus, the threat to cybersecurity generated by the institution is questioning 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). Arguably, organizations ought to embrace effective cybersecurity risk management processes.

Cybersecurity risk management in higher education institutions comprises guidelines, roles, execution, and monitoring (Hommel et al., 2015). Hence, recognize the significance of managing cybersecurity risk to higher education institutions. This study aims to discover more about cybersecurity risk management methods in Malaysia's higher education institutions. It recommends a risk management framework for universities that can assist the management in decision making. This paper is organized as follows: Firstly, the background of the study. Secondly, the literature review. Thirdly, the research methodology, the findings, the conclusion, and the findings.

Background of Study

Nowadays, the emergence of intelligent technologies offers a new type of security danger in higher education. Administrators of higher education institutions consider that security is tremendously a critical problem confronted by their institutions (Gordon, 2015).

Universities in the UK hold crucial intellectual property across the study and supplementary academic resources that might be tempting aims for cyber-criminals (Bandara et al., 2014). Universities UK (2013) mentioned that the universities face a collection of cybersecurity threats. These range from broad and focused attempts to obtain helpful information from webs and their users to disruption to the operation of a university web.

Over the last three years, the University of San Francisco has spent a significant amount of money on cybersecurity to prevent the illegal transfer of funds from the university and the theft of student, parent, employee, and alumni data. It is critical to strengthen the development process and other types of interventions. Some universities significantly affect their prestige and bottom line Grajek (2020) Cybersecurity is convoluted and inclined to obfuscate by university sophistication and working environments (Lane, 2007). The practical implementation of cybersecurity habits and hobbies in universities needs a solid foundation to operate. Yet even though the significance of cybersecurity is not vitally integrated.

In the year 2013, Indonesia's university website with domain ac. Id was ranked second next to the government websites attacked by unofficial individual groups. However, the institutions lack resources, encompassing financial and workers, to address these rising needs. Thus, there is an urgent need to match access with security to guarantee higher education institutions' solutions and missions (Gordon, 2015).

However, at ICESI University, the institutions built the model for assessing computer security for software products on the ISO/IEC 15408 general standards standard, recognizing that applications may lack software design documentation for continuous improvement purposes (Chamorro & Pino, 2011). Furthermore, at the University of Castilla-La Mancha, a framework for the Government of Information Security in Cloud Computing, known as ISGcloud, was proposed to describe processes that systematize relevant security aspects (Rebollo, 2014). Therefore, institutions should effectively manage the cybersecurity risks for the success of every single sector, not just higher education.

Literature Review

In cybersecurity, risks are associated with the possibility of threats exploiting the vulnerabilities of the assets or group of information assets. As a result, it causes harm to an organization (ISO/IEC, 2011). The Standards Association of Australia and Standards New Zealand determined that risk management refers to the architecture (principles, framework, and process) of effectively managing risks (ISO/IEC, 2009). It is not a particular concern from organizations' main interests and procedures. Risk management is a management requirement and an essential component of organizational policies, encompassing critical checking and all responsibility and management processes ("Indian Standard Risk Management — Principles and Guidelines," 2009).

Furthermore, according to the international standards office ISO/ IEC 27005, risk management synchronized activities to shorten and control risks in the organization (ISO/IEC, 2011). It is usually completed by using a specific cybersecurity management system (Clinch, 2009). However, the lack of recognition of the necessity for an employee to be alert to cybersecurity threats for training in safe work practices, principally about maintaining the privacy and confidentially of clients, is the main issue in managing risk (Mubarak, 2016).

Based on the reviews of Grama & Dahlstrom (2016), the awareness of cybersecurity and training programs of higher education institutions are usually taken care of by managers who attend training and awareness responsibility. As a result, higher education institutions' cybersecurity awareness programs are less mature than counterparts in other industries. However, the majority of institutions track awareness program metrics to report. Additionally, the study highlighted that higher education institutions' cybersecurity awareness programs tend to be weak and have small budgets; the program is designed opportunistic (Grama & Dahlstrom, 2016).

Cybersecurity managers in higher education institutions use cybersecurity awareness to strengthen voters with access to sensitive information (Vucetic, 2016). But, there is room for additional coverage on official cybersecurity awareness programs and potential calls to try alternative training methods to reduce events and impacts of security breaches. The factors and definitions of cybersecurity awareness are not used consistently in scientific theories (Vucetic, 2016). Maintaining high-quality teaching resources, meeting the needs of diverse students, and incorporating learning assessment cycles are additional challenges (Ahmad & Maynard, 2014).

However, analysis results show no statistically significant relationship. Besides, it is noted that colleges and universities widely use information security policies, but safety awareness training is not widely used by higher education institutions (Waddell, 2013). In 2016, CIO, CISO, IT directors, managers, and staff all agreed that the provision of cybersecurity education and training is a strategic cybersecurity issue (Grama & Dahlstrom, 2016). Therefore, as shown in a subset of university students, risk perceptions and attitudes may affect industry-standard safety information training (Anzaldua, 2016).

Three of the four institutions surveyed, according to Gordon (2015), have a newly created Information Security Officer role. However, there is no agreement on the chief information security officer (CISO), as most firms that hire a CISO for the first time have the CISO report to either the Chief Executive Officer or the Chief Information Officer (Karanja, 2017).

Higher education institutions' IT instructors are very stable; nearly half of the IT workforce is considering pursuing employment outside their current institution in the years to come (Karanja, 2017). Hence, the quality of life is the most critical factor in keeping IT employees at their present institution (Karanja, 2017). Many higher education institutions, for example, appoint information chiefs (CIOs) at the level of one vice president. The post decided to introduce the role of information security chiefs (CISOs) either as a dual role for the CIO or assign, for example, an IT department head or security expert in a managing locale as CISO, reporting directly to the CIO. In supplement to the official obligations attached to the CISO position, it is a peripheral role within IPT management, management, and operation of IT services, IPT internal users, and distinct interest groups of organizations and public authorities such as law application (Karanja, 2017).

The use of IT resources presents organizations with necessary protection trials because of company procedure connectivity, countless entities that interact alongside IT resources, and the producing intricacy and vibrant nature of IT protection menaces (Karanja, 2017). Therefore, most security measures, standards, and best habits are technical and inadequate for human aspects, even though there are forceful facts that workers are the feeblest link in IT security (Siponen, 2000; Bricki & Green, 2007). According to Hommel et al (2015), the German Federal Information Security Information Bureau (BSI) and its standard document BSI 100-X provides the IT-Grundschutz BSI Methodology also determines the procedure of cybersecurity management. It established a more straightforward risk management approach, which begins with an organizational structured ICT organization analysis for becoming protection requirements.

But for ISO/IEC (2011), this best work orientation reduces the power consumed on menaces and chance identification and their assessment across the meaning of a distinct threat catalog coupled alongside a catalog delineating appropriate security controls (Hommel et al., 2015). In supplement, the US-American National Institute of Standards and Technologies (NIST) provides a risk management way described in NIST SP 800-30 and NIST SP 800-39 different publications.

Research Methodology

This paper is based solely on qualitative data as primary data and secondary data from the review and analysis of the literature. The choice of qualitative method was vital as it served the researcher as an instrument for collecting data by interviewing participants from Malaysian higher education institutions. It utilized multiple case studies to gather data from higher education institutions in Malaysia that allowed to meet the objective of this study. The second method used will be to collect and analyze the data from the literature. It will be conducted by using the Google search engine and the databases. Key terms such as 'cybersecurity risk management in Malaysia Universities' and 'cybersecurity risk management in Malaysia education institutions' will be used. The institutions will find a limited amount of information.

Sample Size

This research will consider the qualitative research method due to the need for the researcher's get a response from professionals in cybersecurity risk management regarding the current process used in educational institutions. According to Hanson et al (2011), the themes in the qualitative research method are confirmed with a sample size of 10 to 20 participants. Thomson (2011), noted that sample size is said once the theoretical saturation is met, and the researchers can only evaluate it throughout the data collection procedure. The sampling frame of this study is drawn from 10 accredited public universities in Malaysia. Therefore, this study will focus on the ten public universities in Malaysia out of 20 universities. The interviewing sessions will meet the specified sample size and achieve adequate data saturation.

Data Collection Method

In this study, the interview method will be conducted with selected experts (cybersecurity risk management) to receive feedback on their current cybersecurity risk management methods. The researcher will begin by identifying participants who met the requirement of the study. The researchers will send an invitation letter to participants via email and WhatsApp. After accepting to participate in the research, the researchers sent the interview protocol with the consent letter. The researchers will use the semi-structured interview to pose questions. the researchers will record the interview by utilizing a smartphone. The researcher will take notes of the perceptions, sentiments, thoughts, and interviewees' facial expressions (Rebollo, 2014). The researcher will use a smartphone audio recorder to record all interviews. After the discussions, the researcher will transcribe the audio recordings. After writing the whole interview transcript, the researcher-led the member's checking process to guarantee that participants still recalled their responses to the questions.

Data Analysis

In this study, separate interviews will be tape-recorded and transcribed. The researcher will first use auto-code after formatting the transcripts into paragraph style with a header. Then the researchers will run the codes into NVivo 12 software which will generate the themes and subthemes for the first time. The second step will be a deep manual analysis of the resulting articles from the auto-coding. This stage will eliminate and group some themes to produce and categorize them based on the study's research questions. According to Bricki & Green (2007), the thematic analysis looks at all data to recognize common problems and distinguishes the main themes that combine all collected data. It is the most available method for qualitative projects that illustrate. Therefore, the researchers will categorize the data into a collection of code, subthemes, and themes.

Findings

The result of this study revealed that literature helped to understand the topic of this paper from the finding of previous studies. Ahlan & Arshad (2012) presented the summary risk framework for a public university. The framework contains all preliminary information about the context, approach, controls, business processes, and assets. Internally from the risk management project, the risk management processes and workflows were designed while referencing relevant international standards. While top management recognizes the university's information and communication technology risks and security, all business processes must always support the implemented policies and initiatives. The final risk framework developed for the IIUM case is depicted in Figure 1.

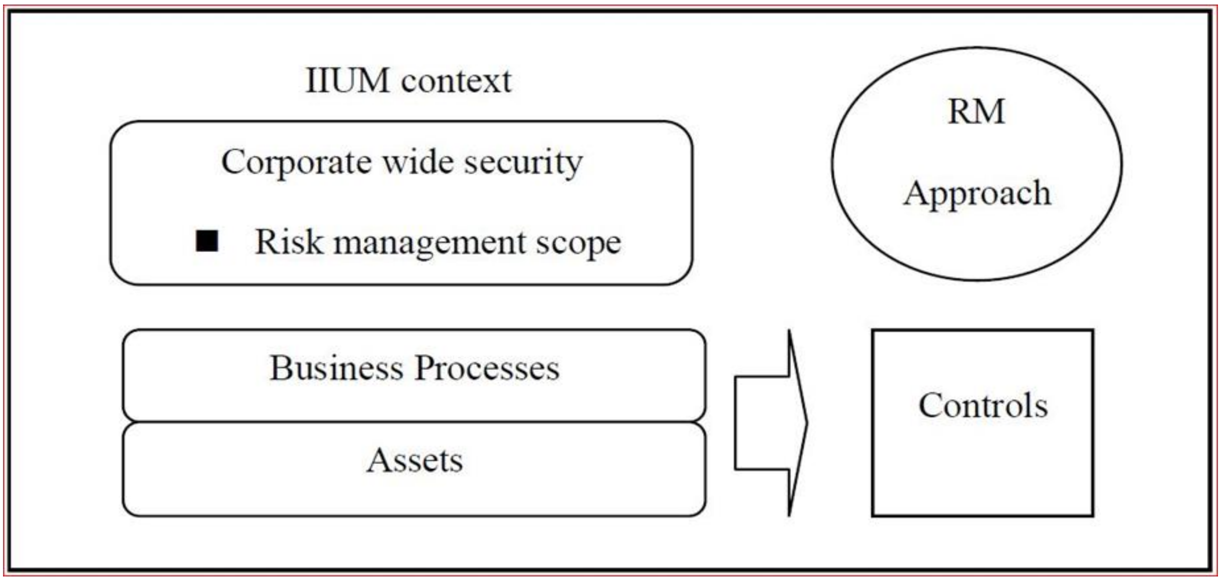


Figure 1: IIUM IT risk management framework
Source: Ahlan & Arshad (2012)

According to Faris et al (2014), URMIS (Universities Risk Management Information System) is a cybersecurity toolkit that provides policies and guidelines for achieving effective cybersecurity risk management in university information systems. To perform the duty of cybersecurity risk management, URMIS must collect data on the status of the information asset, identify different types of risk, and perform risk management duties by a well-defined risk management methodology. In other words, the URMIS work environment consists of knowledge, data, processes, and strategies. However, knowledge, data, process, and procedure are all resources with varying degrees of formalization, and designing an interface for each is difficult. Because of its advantages, this work is based on the multi-agent systems approach. It includes collaboration, complex problem resolution, modularity, efficiency, dependability, and security. Figure 2 illustrates the architecture of URMIS.

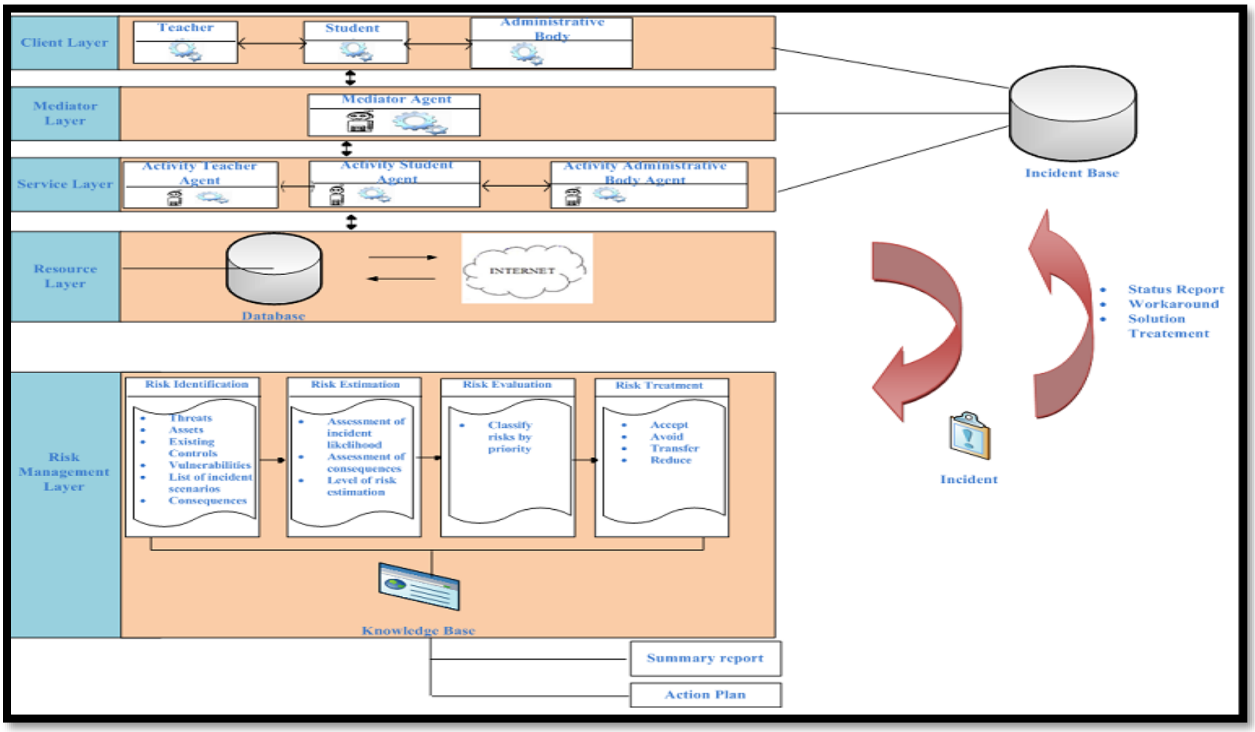


Figure 2: The architecture of URMIS
Source: Bandara et al (2014)

Further, Bandara et al (2014) indicated the way several shareholders (staff and consumers) donate to and are affected by a good management approach to cybersecurity in higher education. Identification and specification necessities represent the input (from the left) to the process cycle with the plan, implementation, evaluation, and maintenance (Bandara et al., 2014). The Control Cycle continues, repeating and continuing the suitable adjustments and iterations, in reply to available information and intelligence. The output (on the right) is a managed security system. Effective adoption of stakeholders, with clear direction and the hopes communicated by management on consumer responsibilities and comportment, is necessary to achieve the safety model.

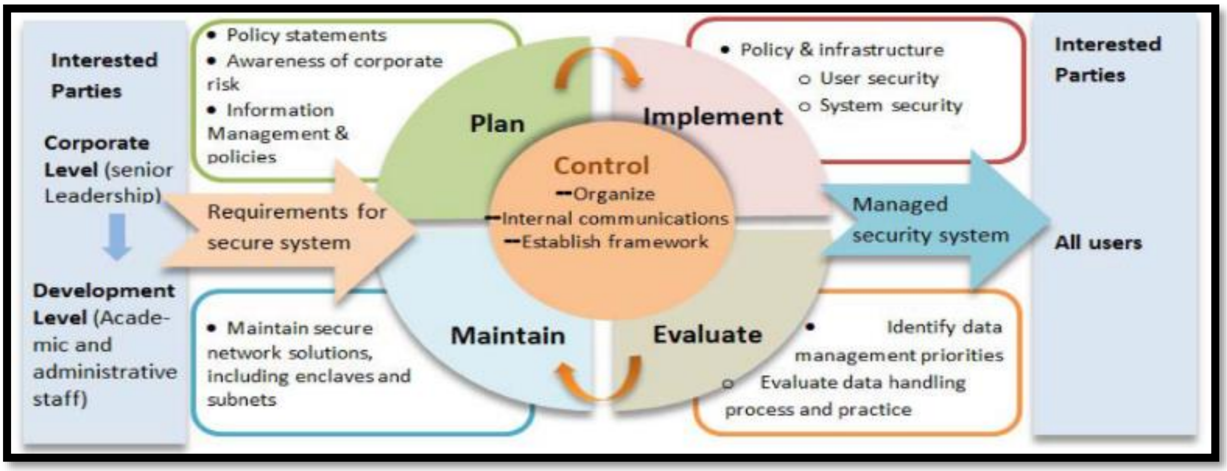

Interested Parties
Corporate Level (senior Leadership)
Development Level (Academic and administrative staff)
Policy statements
Awareness of corporate risk
Information Management & policies
Requirements for secure system
Plan
Implement
Control
—Organize
—Internal communications
—Establish framework
Maintain
Evaluate
Policy & infrastructure
User security
System security
Managed security system
Maintain secure network solutions, including enclaves and subnets
Identify data management priorities
Evaluate data handling process and practice
Interested Parties
All users

Figure 3: The Management of cybersecurity threats in higher education institutions: A process model for the security system
Source: Bandara et al (2014)

As illustrated in Table 1, the risk management components considered by HEIs consist of Alpha, Beta, Chi, dan Delta. The university remains to be the main contributor to churning technical expertise (Ismail et al., 2010).

Table 1: Main Components Considered by HEIs
Source: Ismail et al (2010).

HEI	Components Considered	Standard Adopted
Alpha	Risk Assessment Physical and Environment Security Access Control Information Security Incident Management Compliance	COBIT & ISO 27001
Beta	Risk Assessment Security Policy Organization of Information Security Asset Management Human Resource Security Physical and Environmental Security Communication and Operation Management Access Control Information Systems acquisition, development, and maintenance Information Security Incident Management Compliance	ISO 27001
Chi	Management Safeguards Basic Operations Technical Operations	MyMIS
Delta	Management Safeguards Basic Operations	MyMIS

Hence, this study summarized current InfoSec policy practices. With this and the component considered in Table 1, the study proposes a conceptual framework appropriate for Malaysian HEIs. ISO 27001, MyMIS, and COBIT were used to identify the conceptual framework ISF constructs for HEIs. The established guidelines developed the cybersecurity framework concept, as shown in Figure 4. the researchers identified five primary constructs based on the four (4) interviews to be considered in the HEI ISF. Cybersecurity policy, risk management, access control, an awareness program and training, and compliance are all aspects of cybersecurity. Figure 4 depicts the proposed ISF's conceptual components and associated constructions.

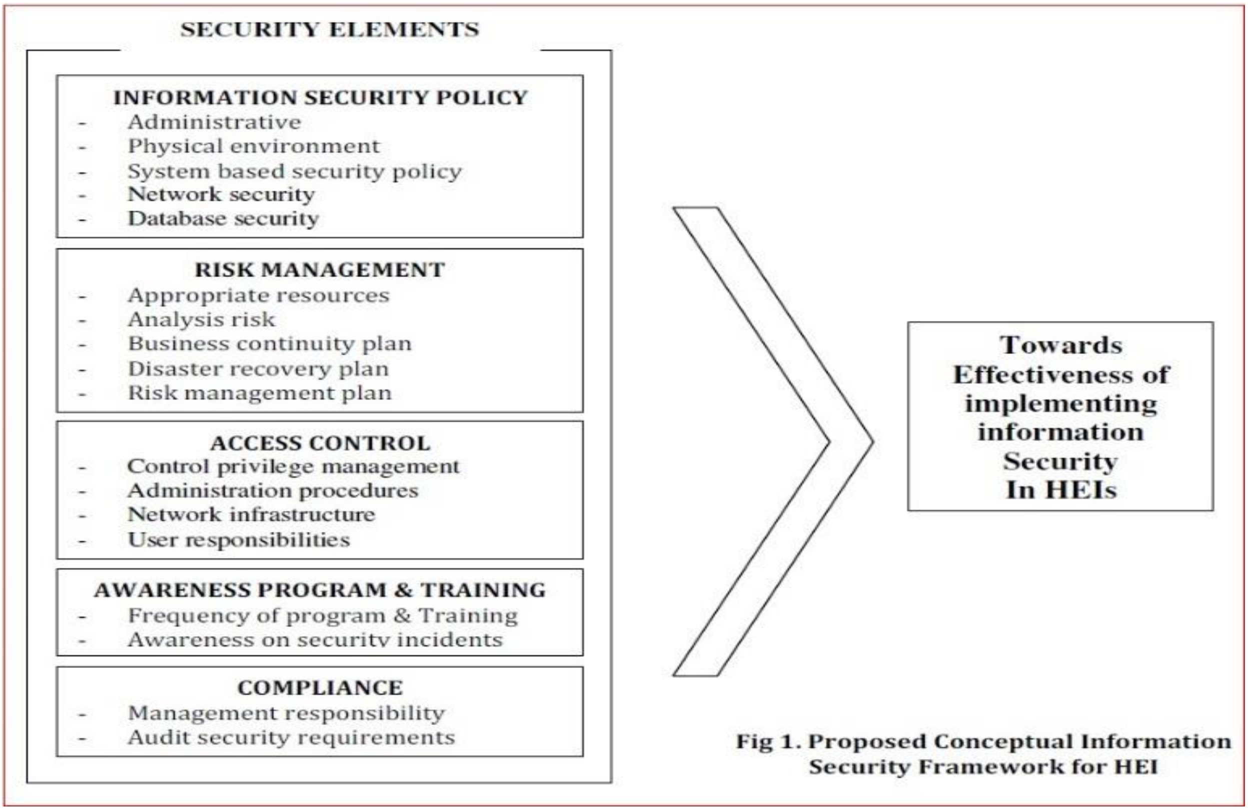

SECURITY ELEMENTS
INFORMATION SECURITY POLICY
- Administrative
- Physical environment
- System based security policy
- Network security
- Database security
RISK MANAGEMENT
- Appropriate resources
- Analysis risk
- Business continuity plan
- Disaster recovery plan
- Risk management plan
ACCESS CONTROL
- Control privilege management
- Administration procedures
- Network infrastructure
- User responsibilities
AWARENESS PROGRAM & TRAINING
- Frequency of program & Training
- Awareness on securitv incidents
COMPLIANCE
- Management responsibility
- Audit security requirements
Towards Effectiveness of implementing information Security In HEIs
Fig 1. Proposed Conceptual Information Security Framework for HEI

Figure 4: Proposed Conceptual Information Security Framework for HEI
Source: Ismail et al (2010).

According to ISO/IEC (2018), figure 5 demonstrates a cybersecurity risk management approach that begins with constructing the context before doing the risk assessment. If the procedure generates enough information to effectively establish the actions needed to reduce the risks to an acceptable level, the work is finished, and risk treatment can begin. If the information is insufficient, an additional iteration of the risk assessment is performed on a subset of the entire scope in conjunction with a changed context (e.g., risk evaluation principles, risk agreement principles, or encounter criteria).

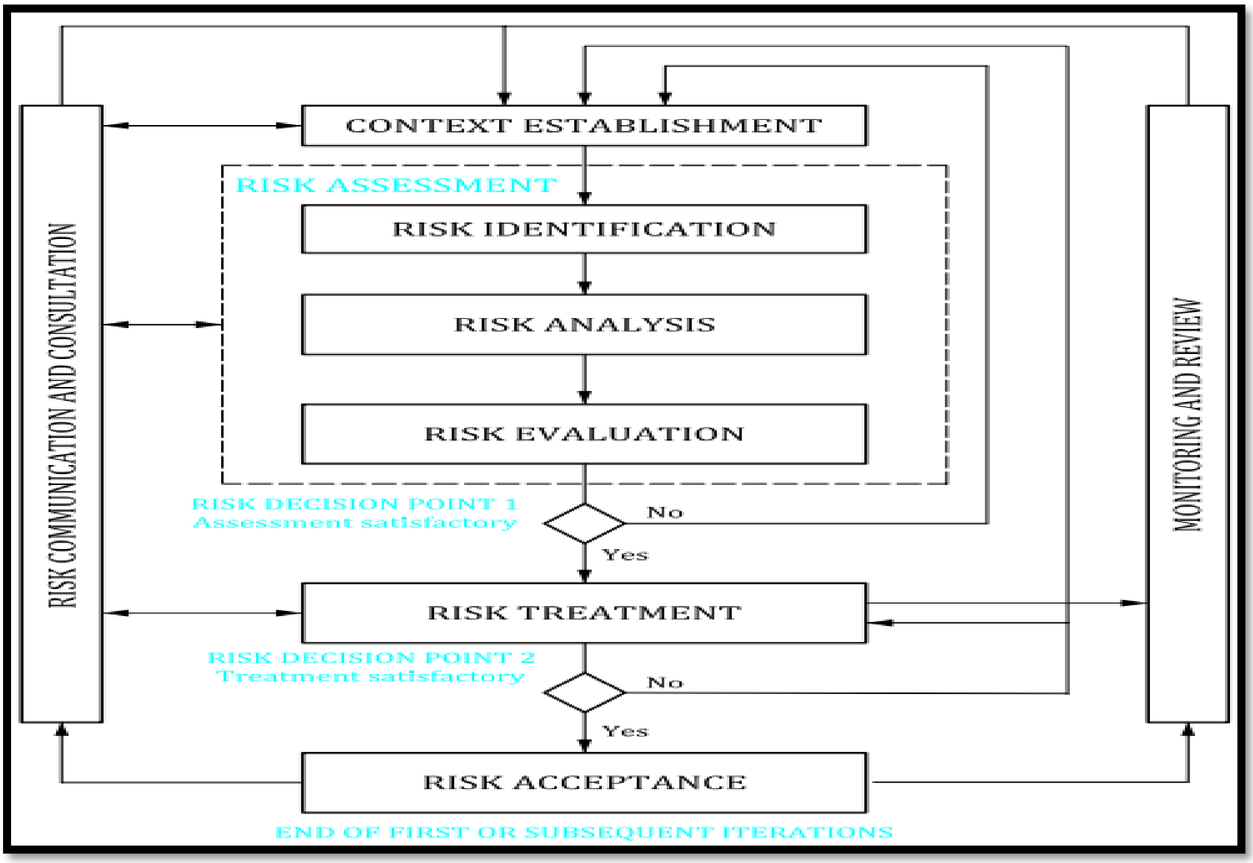


Figure 5: Illustration of an information security risk management process
Source: ISO/IEC (2018)

Conclusion and Future Direction

This study makes the case that risk is not limited to large corporations or non-profit government agencies but that higher education institutions face a slew of cybersecurity threats. However, compared to the rest of the corporate world, Malaysian universities' risk management practices are less developed. The findings highlighted the frameworks and practices in Malaysian education institutions that have contributed to the higher education institutions' cybersecurity risk management process regarding the operation. Based on the review of the existing framework, this study proposes an updated cybersecurity risk management framework.

The proposed framework will address the weaknesses of the current risk management processes in higher education institutions. Besides, it could serve as a model for implementing more robust and long-term information security policies in universities. It is a resource for improving or developing a policy management program. The study will be helpful to the national system as it enhances the security of effective practice. Hence, implementing a customized framework regarding the university's environment will be beneficial as it will manage cybersecurity risk for the well-forming executive. This paper's final research will result in the publication and validation of the proposed framework. Therefore, if the proposed framework is implemented through an application system that contributes to budgets and allows them as a self-assessment tool of their cybersecurity risk. This study calls for further research in cybersecurity-related risk management in the educational system.

References

Gordon, C. J. (2015). Addressing Security Risks for Mobile Devices: What Higher Education Leaders Should Know by Presented to the Faculty of the Graduate College at the University of Nebraska In Partial Fulfillment of Requirements For the Degree of Doctor of Philosophy Major

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.

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

Kang, C. M., Josephng, P. S., & Issa, K. (2015). A study on integrating penetration testing into the information security framework for Malaysian higher education institutions. 2015 International Symposium on Mathematical Sciences and Computing Research, iSMSC 2015 - Proceedings, 156–161.

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, (Itng), 802–804.

Siponen, M. T. (2000), “Critical analysis of different approaches to minimizing user-related faults in 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.

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

Bustamante, F., Fuertes, W., Diaz, P., & Toulkeridis, T. (2016). A methodological proposal concerning to the management of information security in Industrial Control Systems. 2016 IEEE Ecuador Technical Chapters Meeting (ETCM), 1–6.

Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. Journal of Information, Communi, cation and Ethics in Society, 14(3), 254–271.

Grama, J. L., & Dahlstrom, E. (2016). Higher Education Information Security Awareness Programs.

Waddell, S. A. (2013). A Study of the Effect of Information Security Policies on Information Security Breaches in Higher Education Institutions. ProQuest LLC, 190.

ISO/IEC. (2018). Information technology — Security techniques — Information security risk management, ISO/IEC 27005:2018 (E). Joanna Grama. (2017). Understanding IT GRC in Higher Education: IT Risk | EDUCAUSE.

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

ISO/IEC. (2011). Information technology — Security techniques — Information security risk management. Retrieved from http://nsa.wkall.se/litteratur /iso_iec_27005-2011.pdf

ISO/IEC. (2009). Standard Risk Management — Principles and Guidelines on Implementation.

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

Vucetic, S. R. W. J. (2016). Information Security Awareness in Higher Education: A Qualitative Case Study Investigation, (August).

Ahmad, A., & Maynard, S. (2014). Teaching information security management: reflections and experiences. Information Management & Computer Security, 22(5), 513–536.

Anzaldua, J. R. (2016). Does Information Security Training Change Hispanic Students' Attitudes toward the Perception of Risk in the Management of Data Security (Doctoral dissertation, Northcentral University)

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. Information and Computer Security, 25(3), 300–329.

Pomerantz, J., & Brooks, D. C. (2016). The Higher Education IT Workforce Landscape, 2016. Educause Review.

Bricki, N., & Green, J. (2007). A guide to using qualitative research methodology.

Ahlan, A. R., & Arshad, Y. (2016). Information Technology Risk Management: The case of the International Information Technology Risk Management: The case of the International Islamic University Malaysia, (June 2014).

Faris, S., Medromi, H., Hasnaoui, S. El., Iguer, H., & Sayouti, A. (2014). Toward an effective information security risk management of universities' information systems using multi-agent systems, ITIL, ISO 27002, ISO 27005. International Journal of Advanced Computer Science and Applications, 5(6), 114–118.

Bandara, I., Ioras, F., & Maher, K. (2014). Cyber Security Concerns in E-Learning Education. Proceedings of ICERI2014 Conference, (November), 728–734.

Ismail, Z., Masrom, M., Sidek, Z. M., & Hamzah, D. S. (2010). Framework to Manage Information Security for Malaysian Academic Environment, 2010.

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

Lane, T. (2007). Information security management in Australian universities - an exploratory analysis. January, 269.

Chamorro, J., and Pino, F. (2011). Modelo para la evaluación en seguridad informática a productos software, basado en el estándar ISO/IEC 15408 common criteria Sistemas & Telemática 9(19) 69–92

Hanson, J. L., Balmer, D. F., & Giardino, A. P. (2011). Qualitative research methods for medical educators. Academic pediatrics, 11(5), 375-386.

Thomson, S. B. (2011). Research Note Research Method / Research Note. Joaag, 5(1), 45–52.

Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. BMC Medical Research Methodology, 13, 117.

Martínez, R. O. (2014). Marco para el Gobierno de la Seguridad de la Infornación en servicios Cloud Computing.