East African Journal of Education and Social Sciences
EAJESS May –June 2023, Vol. 4, No. 3, pp.229-239
ISSN: 2714-2132 (Online), 2714-2183 (Print). Published by G-Card
DOI: https://doi.org/10.46606/eajess2023v04i03.0294.

Assessment of Higher Education Information Security Risk Management Practices in Tanzania

Fatma Said Kombo
ORCiD: https://orcid.org/0009-0006-3655-9967
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
Email: fatma.kombo@nit.ac.tz

***Peter Godwin Mwakalinga**
ORCiD: https://orcid.org/0009-0006-1199-8074
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
Email: peter.godwin@nit.ac.tz

Lazaro Inon Kumbo
ORCiD: https://orcid.org/0000-0002-6375-9992
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
Email: kumbop@gmail.com

Leticia Mihayo Edward
ORCiD: https://orcid.org/0009-0006-2537-6348
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
Email: mihayoleticia@gmail.com

Neema Phillip Bhalalusesa
ORCiD: https://orcid.org/0009-0002-9113-5586
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
Email: nbhalalusesa@gmail.com

Corresponding Email: peter.godwin@nit.ac.tz

Abstract: This study assessed the information security risk management practices in in Tanzanian Higher Education Institutions (HEIs). It employed the sequential explanatory research design. Out of 51 HLIs in Tanzania, the study selected 10 HEIs from Dar es Salaam. The researchers computed the sample estimation through the Cochran's formula for large population with a precision level of ±10 percentage and confidence level of 95%. The actual sample size was 96 ICT professionals in terms of ICT directors, network administrators, system administrators, ICT support staff and lecturers of ICT. The study used a closed-ended questionnaire, which had Yes/No questions and a structured interview, which collect qualitative data. Quantitative data analysis from the questionnaire was done through descriptive statistics using the SPSS whereas qualitative data from interviews was analyzed using the thematic analysis approach. The study uncovered a notable absence of risk management frameworks and inadequate integration of procedures within institutional strategies. While some HEIs demonstrated effective safeguarding of sensitive information, others required enhancements. The study recommend that HEIs should establish formal risk management frameworks and integrate them strategically into institutional plans. To bridge the implementation gap, HEIs should prioritize comprehensive training, require management support and tailor practices according to their specific contexts.

Keywords: Information Security Risk Management; Higher Education Institutions; Information Security; Information systems.

How to Cite: Kombo, F. S., Mwakalinga, P. G., Kumbo, L. I., Edward, L. M., and Bhalalusesa, N. P. (2023). Assessment of Higher Education Information Security Risk Management Practices in Tanzania. East African Journal of Education and Social Sciences 4(3)229-239. DOI: https://doi.org/10.46606/eajess2023v04i03.0294.

Introduction

The rapid growth of Information and Communication Technologies (ICT) has necessitated Higher Education Institutions (HEIs) to incorporate the use of Information Systems (IS) in various institutional workflows. Among other things, HEIs use ICT in the teaching and learning processes and in managing information about students and staff, finances, research, publication and academic records. The use of ICT in HEIs has, however, elevated information security issues due the increase in number of IS security attacks (Kiura & Mango, 2017; Wang & Chen, 2023). For instance, making institutional network access open to students and visitors has led the increased of unauthorized access and disclosure of sensitive HEIs information. Moreover, IS risk incidents involving data breach or impairment of data integrity have been reported in different HEIs worldwide (Burd, 2006; Candiwan et al., 2016; Nie & Dai, 2017; Garcia & Martinez, 2022), causing reputational harms and financial losses. Burd (2006) found that an estimate of $167,713 is lost on recovering a single security incidence. In Tanzania, there have been reports of cyber-attacks on HEI Information Systems, causing fraudulent use of data and Denial of Service (DoS) attacks (Kundy & Lyimo, 2019; Nfuka et al., 2014). Therefore, leaving HEI's sensitive information unprotected could result to data corruption, loss or misuse by third party, identity theft and public embarrassment.

Information security aims to implement suitable control measures for eliminating or reducing the impacts of different security related vulnerabilities and threats. In particular, information security measures ensure confidentiality, integrity, availability and non-repudiation of information (Zarei & Sadoughi, 2016). The Information Security Risk Management (ISRM) process provides specifics of how information security can be effectively implemented in institutions (Fenz et al., 2011). ISRM is a structured and continuous process of identifying, reviewing, evaluating and monitoring risks to attain an appropriate level of risk acceptability in information systems (Wangen & Snekkenes, 2013). A well-functioning ISRM process influences best InfoSec practices. Successful implementation of ISRM reduces negative risk impacts and ensures that an organization concentrates on high-risk areas, which are managed by using appropriate risk control measures. ISRM also helps the organization to perform cost-benefit analysis of implementation of security controls to ensure a successful InfoSec program (Smith & Brown, 2021).

ISRM is particularly important for higher learning educational institutions, which are increasingly reliant on technology to support their academic, research and administrative functions. Benefits of using ISRM in HEIs include protecting sensitive data, preserving academic and research integrity, ensuring regulatory compliance and promoting a culture of security awareness. For example, a study by Reegård et al. (2019) found that implementing a risk management framework helped a HEI in Oman to identify and mitigate potential security threats, thereby protecting sensitive data and preserving academic and research integrity. Similarly, a study by (Maneerattanasak & Wongpinunwatana, 2017) found that effective risk management can help HEIs comply with regulatory requirements and standards. A study by (Sum & Zurina, 2017) showed that promoting a culture of security awareness among students, faculty and staff can help to reduce the likelihood of security breaches and improve the overall security posture of HEIs.

Despite its benefits, there are still challenges related to how ISRM is practiced in HEIs. ISRM activities are still in the infant stages of formalization in HEIs compared to other type of institutions (Bongiovanni, 2019; Pastwa et al., 2016). However, little is known about specific challenges facing the ISRM implementation in HEIs in African countries. This affects the ability to deploy appropriate strategies for ISRM practices. For example, Bakari et al., (2005) assessed the state of InfoSec and risk management in HEIs in Tanzania and found a mismatch between ISRM practices in Tanzanian HEIs and the recommendations in international risk management standards. Hence, this study sought to investigate the Information Security Risk Management practices in HEIs in Dar es Salaam, Tanzania.

Literature Review

HEIs face numerous challenges on how to make informed assessment of reputational, legal and financial risks posed by unauthorized access or disclosure of information (Alshaikh, 2018; Ahlan & Arshad, 2012; Hommel et al., 2015). They also grapple with ineffective means of implementing technical security controls, which fail to address specific needs of the institutions and lack of cost-

benefit analysis on implementation of such controls (Hassen & Zakaria, 2013; Tixteco et al., 2017; Wagiu et al., 2019). ISRM practices, which adhere to the available standards assist in setting out specific strategic processes for identifying all the risks associated with the use of IS and promote mitigation of such risks in order to improve institutional information security. Studies on ISRM have focused on the protection of information assets through technical controls but have not paid enough attention to its practicability (Bergström et al., 2019). Without proper understanding of ISRM practices, securing information can be particularly challenging. For instance, if information risks are not adequately identified, poor security controls are likely to be developed because development of good security controls depends on accurate procedure for risk identification, assessment and analysis.

Different authors have identified ISRM implementation challenges in HEIs (Ahlan & Arshad, 2012; Ates & Gunes, 2018; Bergström et al., 2019; Hassen & Zakaria, 2013; Kiura & Mango, 2017). Hassen and Zakaria (2013) reported the lack of extensive implementation of risk management standards in many HEIs. Failure to comply with the approved standards and laws for risk management was found to be among the main challenges among universities in Turkey, resulting in limited use of risk identification and analysis procedures (Ates & Gunes, 2018). Lack of adequate knowledge and experience to conduct ISRM activities was found to be another challenge facing the implementation of ISRM in HEIs. Despite the fact that IT personnel are aware of the importance of ISRM, there is lack of on-job training to support ISRM practices and improve risk evaluation (Ahlan & Arshad, 2012; Ismail et al., 2014). Failure to identify sources of threats and vulnerabilities is another major challenge in ISRM practice in HEIs. This is caused by lack of detailed internal guidelines for the ISRM process (Webb et al., 2014). Additionally, managers in HEIs experience a challenge of recognizing and administering information security risks across their institutions due to lack of proper guidance on effective ISRM programs for controlling how the institutions should manage and respond to information security risks. Due to the rapid growth of ICT, it is impossible to eliminate all security incidences, but adhering to systematic procedures for ISRM can help to reduce security incidences and protect information security assets in institutions (Bolek et al., 2016).

Other studies focused on the use of risk management frameworks to improve ISRM practices in HEI (Ahlan & Arshad, 2012; Hassen & Zakaria, 2013; Kiura & Mango, 2017; Sultan et al., 2014). However, such frameworks do not provide practical guidance to enhance the ISRM practices. As a result, little is known about how HEIs can, in practice, ensure effective protection of their information systems (Bergström et al., 2019). Ahlan and Arshad (2012) proposed a risk management framework focusing on improving ISRM procedures on risk assessment and risk treatment planning. A similar study was conducted by Kiura and Mango (2017) who adopted ISO 27005 to propose a risk management model that covers strategy, technology, organization, people and environment view of ISRM.

ISO/IEC 27005 represents an International Organization for Standardization (ISO) intended to provide guidance for information security risk management. It supports the general concepts specified in ISO/IEC 27001 to implement information security through a risk management approach. ISO/IEC 27005 focuses on ISRM to determine the risk impact and likelihood to the information asset from threats and vulnerabilities that exist. Different studies (Alwi et al., 2019; Sultan et al., (2014); Candiwan et al., 2015; and Zarei & Sadoughi, 2016) adopted ISO 27005 standards for analyzing, assessing and managing risk in different information systems. The adoption ISO 27005 ISRM standard is due to its flexibility in the risk assessment process, usability and provision of continuous flow of the risk management process (Alwi et al., 2019).

The methodology splits risk management process into three phases; context establishment, risk assessment and risk treatment (Hommel et al., 2015; Alcántara & Melgar, 2015). Figure 1 shows the overview of the ISRM process as specified in the ISO/IEC 27005:2011. This methodology will be used in this study to establish the extent that HEIs in Dar es Salaam practice ISRM.

Moreover, to improve ISRM practices, various standards have been used to propose different methods for risk assessment (Candiwan et al., 2015; Hommel et al., 2015; Sultan et al., 2014; Suroso et al., 2018; Tixteco et al., 2017; Wagiu et al., 2019). However, the existence of many standards for ISRM makes institutions to be uncertain regarding what standard is more effective to use. Since there is no a one-size-fits-all solution, it is necessary to adopt a risk management standard that addresses the needs of a specific institutions (Ahmad& Mohammad, 2012). Dutiful adoption and the comprehensiveness of a standard helps to ensure that risks are managed effectively and efficiently across institutions. A comprehensive and well-structured risk management procedure that consists of different sets of activities can therefore be adequately used in HEIs.

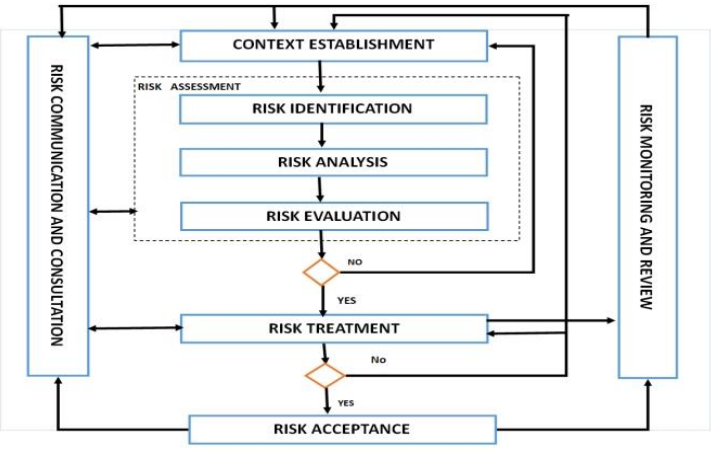

Figure 1: Information Security Risk Management Process (ISO27005, 2011)

The existing challenges present various opportunities for enhancing ISRM practices in HEIs. The comparative analysis of information security risks among universities in Turkey found the possibility of increasing InfoSec in HEIs by providing training and security risk management procedures to employees (Yilmaz & Yalman, 2016). The analysis shows that HEIs had a level of security awareness, some certified professionals and resources like time, personnel and budget. Alshaikh (2018) reported the successful implementation of ISRM practices in other organizations where there are formal approaches and compliance with standards and regulatory requirements. Apart from what is described in risk management standards, the risk management process can benefit from the practices formed by employees' experience and personal ambitions (Fenz et al., 2014). This suggests that apart from complying with security standards, a good ISRM process should be tailored to suit risk management needs of specific organizations since risks occurring in organizations differ from one industry to another.

More specifically, tailoring of risk management standards to HEIs strongly depends on clear understanding of the practical challenges facing risk management practitioners in such institutions. However, to the best of the researchers' knowledge, little is known about these challenges in the context of African countries. This continues to threaten the security of sensitive information maintained by HEIs

Methodology

Design

This study adopted a sequential explanatory research design, which aims at obtaining a comprehensive and in-depth findings, grounded in respondents' experience. This approach ensures a more holistic understanding of the subject matter. It enabled the researchers to, not only uncover prevailing trends, but also to explore the intricate contextual elements specific to HEIs in Dar es Salaam. These insights can then be used to enhance and focus risk management practices within the higher education sector, making them more effective and tailored to the local environment.

Population and Sampling

Out of 51 higher learning institutions in Tanzania (TCU, 2020), the study selected 10 HEIs from Dar es Salaam, which has about 33% of the HEIs in the country. The selected HEIs include National Institute of Transport, University of Dar-es-salaam, Ardhi University, The Aga Khan University, Hubert Kairuki Memorial University, Open University of Tanzania, St. Joseph University, Tumaini University Dar-es-

Salaam College, Kampala International University and United African University of Tanzania. The researchers computed the sample estimation through the Cochran's formula for large population (Israel, 1992) with a precision level of ±10 percentage and confidence level of 95%. The actual sample size was 96 ICT professionals in terms of ICT directors, network administrators, system administrators, ICT support staff and lecturers of ICT.

Instruments

The study used a closed-ended questionnaire, which had Yes/No questions and a structured interview, which collect qualitative data.

Validity and Reliability

To ensure validity, the instruments were pilot tested with 30 respondents from HEIs who were not included in the real survey. The pilot study results helped to refine the instruments and improve comprehension. Data reliability was determined using Cohen's Kappa Coefficient of 0.671.

Statistical Treatment of Data

Quantitative data analysis from the questionnaire was done through descriptive statistics using the SPSS whereas qualitative data from interviews was analyzed using the thematic analysis approach.

Ethical Consideration

The researchers administered the informed consent to participants before the data collection process. They ensured privacy and confidentiality in order to adhere to ethical guidelines and codes of conduct. Additionally, the researchers reported the findings accurately, transparently and without bias.

Results and Discussion

This section presents results of the study. It starts with presentation of demographics of respondents and then moves into presentation of results through research questions.

Demographics of Respondents

Study findings in table 1 indicates that 19 (22.9%) of respondents were Network Administrators, 16 (19.3%) were ICT Support, 30 (36.1%) were System Administrators, 5 (6%) were ICT Directors and 13 (15.7%) were ICT educators. In terms of education level, six (7.2%) had basic certificates, eight (9.6%) had diplomas, 38 (45.8%) had Bachelors' Degrees, 20 (24.1) had Masters' Degrees and 11 (13.3%) had doctorate degrees.

Table 1: Respondents Demographic Profile (n=83)

Factors	Category	f	%
Job Title	Network Administrator	19	22.9%
	ICT Support	16	19.3%
	System Administrator	30	36.1%
	ICT Director	5	6%
	ICT Educators	13	15.7%
	Total	**83**	**100%**
Education Qualification	Basic Certificate	6	7.2%
	Diploma	8	9.6%
	Bachelor's Degree	38	45.8%
	Master's Degree	20	24.1%
	Doctoral Degree	11	13.3%
	Total	**83**	**100%**
Years of Experience	Below 2	13	15.7%
	From 2 to 4	24	28.9%
	From 5 to 10	37	44.6%
	Above 10	9	10.8%
	Total	**83**	**100%**
Risk Certification	Yes	10	12%
	No	73	88%
	Total	**83**	**100%**

In terms of years of experience, 13 (15.7%) had worked for below two years, 24 (28.9%) had worked for two to four years, 37 (44.6%) had worked for five to 10 years and nine (10.8%) had worked for above ten years. Ten (12%) had received certification while 73 (88%) had not received certification.

Research Question 1: To what extent do HEIs practice ISRM according to the ISO 27005?

This research question sought to establish the extent to which HEIs practice ISRM according to the ISO 27005. Several indicators revealed practices as follows:

Risk Management Implementation

In table 2, majority of the respondents (63.9%) reported that their institutions had not implemented any standard risk management framework for providing general procedures for risk management activities at the institutions. This implies the absence of systematic procedures for ISRM activities at the institutions, which may hinder efficiency of the practice. These findings similar to a study done by Hassen and Zakaria (2013) where only 29.1% of HEIs in Malaysia had adopted risk management standards. Despite the implementation of ISRM practice, most HEIs in the country did not follow the standard practices.

Table 2: Implementation of Risk Management frameworks

SN	Item in the Questionnaire	Yes		No		Don't Know	
		f	%	f	%	f	%
1	Implementation of risk management	5	6	53	63.9	25	30.1
2	Establishing contexts to define risk	7	8.4	54	65.1	22	26.5
3	Risk management team	21	25.3	47	56.6	15	1.1

Table 3: Procedure for Risk Identification (n=83)

Item in the Questionnaire	Yes	No	Don't Know
There is procedure for ICT assets identification	36.1%	45.8%	18.1%
There is a procedure to identify system vulnerabilities	16.9%	57.8%	25.3%
All potential threats are identified and documented	21.7%	49.4%	28.9%
There are risk controls identification procedures	27.7%	51.8%	20.5%

Context Establishment to Define Risk

In order to practice ISRM successfully, context establishment is the first step where institutions set strategic plans on how information risk can be managed (Hassen & Zakaria, 2013). Table 2 shows that 65.1% of the respondents had reported that their institutions have not established any context (scope, internal and external) to define InfoSec risks. Furthermore, 26.5% of the respondents reported that they do not know whether the context for risk management was in place. This indicates that there are either no or just limited information risk awareness programs at such institutions, implying that the concept of risk and its impact in institutional objectives is still at infancy stages as explained by Tixteco et al., (2017). The results are comparable to those in the study by Ionescu et al., (2018) on establishing requirements for implementing the information security management system where context establishment was overlooked.

Risk Management Team

The findings in Table 2 further show that most of respondents (56.6%) reported that their institutions do not have risk management teams to undertake information security risk management processes. Lack of risk management teams affects the implementation of ISRM activities in the institutions. A study by Prislan et al., (2017) explained risk management team works with an open mind and enthusiasm towards understanding risk and being able to mitigate it.

Procedure for Risk Identification

Table three shows that minority of respondents agreed that procedures for risk identification, in terms of four statements in the questionnaire, are implemented.

This implies that there is no sequence of sub activities to adequately identify InfoSec risks at the institutions. Systematic identification of ICT assets, threat-vulnerabilities identification, threat documentation and risk controls identification procedures are among the sub-activities in information security risk identification. A study by Zarei and Sadoughi (2016) obtained similar results whereby risk identification procedures were not documented, hence poor risk management.

Risk Treatment and Risk Acceptance

Risk treatment implies putting controls in place and implementing methods to reduce the level of risk in organizations (Stroie & Rusu, 2011). Because it is almost impossible to eliminate all risks, the organization's management needs to implement

measures to lower the risks to an acceptable level and thus reduce the negative impact of the risk on the organization's objectives and goals.

Table 4 shows that minority of respondents agreed about the availability of risk treatment and risk acceptance. The majority either disagreed or did not know about the existence of risk treatment and risk acceptance in their institutions. These results were in line with results by Webb et al., (2014) which assessed risk treatment procedures in small scale enterprises. The study revealed that among SMEs there is a notable tendency for low levels of engagement in risk treatment strategies and a general reluctance towards risk acceptance measures.

Table 4: Risk Treatment and Acceptance (n=83)

SN	Statement in the Questionnaire	Yes	No	Don't Know
1	There is documented risk treatment criteria and plan to reduce, retain, avoid or share the system security risk	21.7%	43.4%	34.9%
2	Risk treatment options are done based on outcome for risk assessment	8.4%	56.6%	34.9%
3	Risk treatment options are done based on the expected cost of security controls	13.3%	49.4%	37.3%
4	There is approach to identify the remaining risk and risk acceptance	-	61.4%	38.6%

Table 5: Risk assessment Procedures (n=83)

	Statement in the Questionnaire	Yes	No	Don't Know
Risk Analysis and Evaluation	Procedure for analyzing Information security risk	19.3%	50.6%	30.1%
	Systematic procedure for evaluating Information security risk	8.4%	72.3%	19.3%
Risk Monitoring and Review	Using systematic procedure to monitor and review InfoSec risk	7.2%	68.7%	24.1%
	There is regular review of compliance of IS with Institutional InfoSec policies and guidelines	39.8%	50.6%	9.6%
Risk Communication and Sharing	There is security risk communication strategy	9.6%	72.3%	18.1%
	Risk management results is shared among ICT stakeholders, top management and other decision makers in the institution	24.1%	59%	16.9%

Table 5 shows the procedures in risk assessment in terms of risk analysis and evaluation, risk monitoring and review and risk communication and sharing.

Risk Analysis and Evaluation

Risk analysis and evaluation present actions for determining priorities in managing the risks based on available funds, deciding what to do for each risk level, depending on risk treatment criteria agreed by the institution. Table 5 shows that 50.6% of respondents had no procedure for analyzing InfoSec risks at their institutions. This implies that scores for risk likelihood and impact were not defined in their institutions, lacking grounds for differentiating risks from problems. Despite the fact that 19.3% of the respondents agreed to have procedures for analyzing information security risks, only 8.4% of the respondents reported having systematic procedures for evaluating risks at their institutions. Similar results were reported by Jones (2020) where HEIs did not set the risk analysis and evaluation criteria. The study suggested that without defining the risk evaluation criteria, institutions could not establish which risks need urgent attention and which risks should be tolerated or avoided.

Risk Monitoring and Review

When there are changes in institutional plans and objectives, some risks are terminated due to changes of business processes while other risks may emerge from technological advancement. Table five shows that 39.8% of the respondents reported that their institutions did the continuous review of information security policies to comply with their information systems. On the other hand, 68.7% of the respondents reported that there is no systematic procedure for monitoring and review of information security risks. This implies the presence of minimal review of compliance with risk management policy frameworks and largely unsystematic risk monitoring and review. The researchers found similar trends in the study by Alshaikh (2018) which described the importance of risk monitoring.

Risk Communication and Sharing

The process of risk communication, consultation and results sharing process should take place at every stage of risk management, from establishing the context to risk treatment. The results in Table 5 show that 59% of the respondents reported that their institutions did not share risk management results among stakeholders. Despite the fact that 24.1% of respondents reported that their institutions shared risk management results, 72.3 % of the respondents reported that their institutions do not have a security risk communication strategy. This implies that it is difficult for stakeholders to have information about risks in order to make informed decisions regarding possible impacts of InfoSec risks. In contrast, the study done by Hassen and Zakaria (2013) found that 51.2% of HEIs in Malaysia have risk communication strategies in their institutions. This is due to well-formulated information security policy and strategic planning on InfoSec and InfoSec culture in the institutions.

Research Question 2: What are current ISRM practices in HEIs?

This research question sought to establish current ISRM practices in HEIs. Through interview, one of respondents revealed that, "We use ICT policy that covers people, procedures and IT resources for managing all systems security. We put security controls to ensure that all information systems are secured." It was further revealed that,

> Training is given mostly to staff on how to use the system. We have a system admin who has all the rights over the system. We normally perform backups depending on the sensitivity of data that may be once a week or after every two to three days.

In addition, the study found that there are a number of information security experts in HEIs bearing roles such as system administrator, chief security officer and ICT security officer who assist in managing the security of information. These security experts ensure security of information in HEIs using different techniques including security awareness training to the staff, data backup procedures, password policy and security auditing of information systems. Such strategies used in protecting information systems are similar to those found by Hassen and Zakaria (2013) and Candiwan et al. (2016).These studies found that organizations employ various risk strategies to protect their information systems, including encryption, access controls and regular security audits. This implies that HEIs are aware of the importance of managing security of their information to prevent any loss due to lack of confidentiality, integrity and availability of information.

The study also found that the available ICT policies do not contain procedures for ISRM (ii) there are no information security risk management guidelines. Furthermore, there are inadequate security controls for protecting information systems. The following interview excerpts resonates with the research findings:

> Apparently, we do not have a specific procedure for InfoSec risk management that is defined in our ICT policy, and I do not think we are using adequate procedures since we are based on the experience of threat events to implement security controls and security procedures to the system.

Another respondent reported that

> One of the drawbacks I can see is the lack of effective means to protect our information systems. Technology is always changing so there are new threats every day that may jeopardize our systems if there are no means to assess the loopholes. Failure to have adequate process or formal guidelines for managing risk can result in failure in protecting our information systems.

These results are similar to those obtained by Zarei and Sadoughi (2016) during assessment of ISRM practices in Iran's Hospitals. The study recommended Iran's ministry of Health to develop practical policies for improving ISRM in hospitals of Iran. Regarding the importance of risk treatment and risk communication in the organization, the literature suggests that HEI are obliged to formulate risk treatment and communication strategies.

The study also found that HEIs have a level of management in ICT security, which plan, coordinate, organize and control ICT security activities. This is crucial for safeguarding sensitive data, ensuring regulatory compliance and maintaining the trust of stakeholders in institutions. It also prevents financial losses, operational disruptions and reputational damage caused by cyberattacks and data breaches Hassen & Zakaria, (2013).

Moreover, even though there are various activities conducted for risk management in most HEIs in Dar es Salaam, such as ensuring effective methods for security of data in information systems, if the activities are not systematically designed, risk assessment and evaluation will not be accurate. ISRM is a continuous process of identification, assessment, evaluation and treatment of risk to an acceptable level. Therefore, the improvement should be consistent across ISRM activities in order to achieve significant risk management results.

Conclusions and Recommendations

Conclusions

The study has uncovered a notable absence of risk management frameworks and an inadequate integration of procedures within institutional strategies. This deficiency suggests a crucial need for standardized risk management approaches to ensure data protection and uphold academic institution integrity. Moreover, the comprehensive assessment of current ISRM practices in HEIs reveals a broad awareness of risk management's significance and objectives. However, there were significant variations in implementation strategies among institutions. While some HEIs demonstrated effective safeguarding of sensitive information, others required enhancements. Enhancing engagement in ISRM activities necessitates a combination of comprehensiveness, management backing and context-sensitive implementations for optimal results.

Recommendations

The study recommend that HEIs should establish formal risk management frameworks and integrate them strategically into institutional plans. To bridge the implementation gap, HEIs should prioritize comprehensive training, require management support and tailor practices according to their specific contexts. Furthermore, sharing best practices among HEIs and other institutions can facilitate the adoption of effective strategies, fostering a collective effort towards safeguarding sensitive information, enhancing risk management practices and upholding the integrity of HEIs.

References

Ahlan, A. R., & Arshad, Y. (2012). Information Technology Risk Management : The case of the International Islamic University Malaysia. Journal of research and Innovation in Information Systems, June 2014, 58–67. Retrieved from http://irep.iium.edu.my/id/eprint/32107.

Ahmad, W. Al, & Mohammad, B. (2012). Can a Single Security Framework Address Information Security Risks Adequately? International Journal of Digital Information and Wireless Communications, 2(3), 222–230. Retrieved from https://link.gale.com/apps/doc/A354578204/AONE?u=anon~cd602e90&sid=googleScholar&xid=4b820da3.

Alshaikh, M. (2018). Information Security Management Practices in Organisations. University of Melbourne, March, 1–294. Retrieved from http://hdl.handle.net/11343/208934.

Alwi, A., & Zainol A, Khairul. A. (2019). Information Security Risk Assessment for the Malaysian Aeronautical Information Management System. Proceedings of the 2018 Cyber Resilience Conference, CRC 2018, 1–4. https://doi.org/10.1109/CR.2018.8626841.

Ates, V., & Gunes, B. (2018). The Factors affecting Information Technologies Risk management at Turkey State Universities. International Journal of Ebusiness and Egovernment Studies, 10(2), 46–62. Retrieved from https://www.scinapse.io/papers/2944124154.

Bakari, J. K., Tarimo, C. N., Yngström, L., & Magnusson, C. (2005). State of ICT Security Management in the Institutions of Higher Learning in Developing Countries : Tanzania Case Study. Fifth IEEE International Conference on Advanced Learning Technologies, 3–7. http://d x.doi.or g/10. 1109/ICALT.2005.243.

Bergström, E., Lundgren, M., & Ericson, Å. (2019). Revisiting information security risk management challenges : a practice perspective. Information & Computer Security. https://doi.org/10.1108/ICS-09-2018-0106.

Bolek, V., Látecková, A., Romanová, A., & Korcek, F. (2016). Factors affecting information security focused on SME and agricultural enterprises. Agris On-Line Papers in Economics and Informatics, 8(4), 37–50. https://doi.org/10.7160/aol.2016.080404.

Bongiovanni, I. (2019). The least secure places in the universe ? A systematic Literature Review on Information Security Management in Higher Education. Computers & Security, 86, 350–357. https://doi.org/10.1016/j.cose.2019.07.003.

Burd, S. A. (2006). The Impact of Information Security in Academic Institutions on Public Safety

and Security in the United States,2005-2006. https://doi.org/10.3886/ICPSR21188.v1.

Candiwan, C., Sari, P. K., & Sebastian, J. (2015). Comparison Analysis of Information Security Risks and Implementation of ISO27001 on Higher Educational Institutions in Indonesia. International Journal of Basic & Applied Sciences, 11(4),40-52.

Candiwan, Kencana, P., & Nursharbina, N. (2016). Assessment of Information Security Management on Indonesian Higher Education Institutions. Lecture Notes in Electrical Engineering, 362, 375–384. https://doi.org/10.1007/978-3-319-24584-31.

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information Security Risk Management: In which security solutions is it worth investing? Communications of the Association for Information Systems, 28(1), 329–356. https://doi.org/10.17705/1cais.0282.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management and Computer Security, 22(5), 410–430. https://doi.org/10.1108/IMCS-07-2013-0053.

Garcia, M., & Martinez, R. (2022). Enhancing Information Security Culture in Universities: A Case Study of Effective Training Programs. Journal of Educational Technology and Cybersecurity, 18(4), 87-101.

Hassen, S., & Zakaria, M. S. (2013). Managing University IT Risks in Structured and Organized Environment. Research Journal of Applied Sciences, Engineering and Technology, 6(12), 2270–2276. https://doi.org/10.19026/rjaset.6.3858.

Hommel, W., Metzger, S., & Steinke, M. (2015). Information Security Risk Management in Higher Education Institutions : From Processes to Operationalization. EUNIS Journal of Higher Education IT, 2015/3. Retrieved from http://hdl.handle.net/11366/448.

Ionescu, R. C., Ilie, C., & Ceausu, I. (2018). Considerations on the implementation steps for an information security management system. Proceedings of the 12th International Conference on Business Excellence, 43(ISSN 2558-9652), 476–485. https://doi.org/10.2478/picbe-2018-0043.

Ismail, W., Norwawi, N. M., & Saadan, K. (2014). The Challenges in Adopting Information Security Management System for University Hospitals in Malaysia. Proceeding of Knowledge Management International Conference (Kmice) 2014, 8(1), 902–907. Retrieved from http://ddms.usim.edu.my:80/jspui/handle/123456789/8990.

Israel, G. D. (1992). Determining Sample Size. University of Florida Cooperative Extension Service, Institute of Food and Agriculture Sciences, EDIS, Florida, November, 1–5. Retrieved from https://www.psycholosphere.com/Determining%20sample%20size%20by%20Glen%20Israel.pdf.

Jones, A. (2020). Information Security Risk Management in Higher Education: Challenges and Strategies. Journal of Higher Education Technology, 25(3), 45-61.

Kiura, S. M., & Mango, D. M. (2017). Information Systems Security Risk Management (ISSRM) Model in Kenyan Private Chartered Universities. European Journal of Computer Science and Information Technology, 5(2), 1–15.

Kundy, E., & Lyimo, B. (2019). Cyber Security Threats in Higher Learning Institutions in Tanzania, A Case of University of Arusha and Tumaini University Makumira. Olva Academy-School of Researchers, 2(3). Retrieved from https://www.academia.edu/40894854/cyber_security_threats_in_higher_learning_institutions_in_tanzania_a_case_of_university_of_arusha_and_tumaini_university_makumira.

Maneerattanasak, U., & Wongpinunwatana, N. (2017). A Study of Success Factors of Principle and Practice in Information Technology Risk Managementt. Proceedings of International Academic Conferences 5407887, International Institute of Social and Economic Sciences

Nfuka, E. N., Sanga, C., & Mshangi, M. (2014). The Rapid Growth of Cybercrimes Affecting Information Systems in the Global : Is this a Myth or Reality in Tanzania ? International Journal of Information Security Science, 3(2), 182–199. Retrieved from http://www.suaire.sua.ac.tz/handle/123456789/1749.

Nie, J., & Dai, X. L. (2017). On the Information Security Issue in the Information Construction process of colleges and universities. Proceedings - 12th International Conference on Computational Intelligence and Security, CIS 2016, 582–585. https://doi.org/10.1109/CIS.2016.140.

Pastwa, A. M., Hommel, U., & Li, W. (2016). The State of Risk Management in Business Schools. Journal of Management Development, Vol. 35(Iss 5), 1–17. https://doi.org/http://dx.doi.org/10.1108/JMD-08-2014-0088.

Prislan, K., Lobnikar, B., & Bernik, I. (2017). Information Security Management Practices : Expectations and Reality. Advances In Cybersecurity 2017, November, 2013–2016. https://doi.org/10.18690/978-961-286-114-8.1.

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In 29th European Safety and Reliability Conference (pp. 4036-4043).

Stroie, E. R., & Rusu, A. C. (2011). Security Risk Management - Approaches and Methodology. Informatica Economica, 15(1), 228–240. Retrieved from https://core.ac.uk/download/pdf/6612749.pdf.

Smith, J., & Brown, L. (2021). An Empirical Analysis of Information Security Practices in Higher Education Institutions. International Journal of Cybersecurity, 12(2), 213-230.

Sultan, S., Maram, A.-J., Mashal, F., & Daas, F. (2014). Developing an ISO27001 Information Security Management System for an Educational Institute : Hashemite University Jordan Journal of Mechanical and Industrial Engineering, 8(2), 102–118. Retrieved from http://jjmie.hu.edu.jo/vol%208-2/JJMIE-37-14-01.pdf.

Sum, R., & Zurina, S. (2017). Risk Management in Universities. 3rd International Conference on Qalb-Guided Leadership in Higher Education Institutions 2017, December. Retrieved from https://www.researchgate.net/publication/321746840_Risk_Management_in_Universities

Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment Of Information System Risk Management with Octave Allegro At Education Institution. Procedia Computer Science, 135, 202–213. https://doi.org/10.1016/j.procs.2018.08.167.

TCU. (2020). Tanzania Commission for Universities List of Approved University Institutions in Tanzania. July1–6. https://www.tcu.go.tz/sites/default/files/list of university institutions in tz as of 30.6.2020.pdf

Tixteco, L. P., Prudente, C., Pérez, G. S., Toscano, L. K., Jesús, J. De, Gómez, V., De, A., & Tellez, C. (2017). Recommendations for Risk Analysis in Higher Education Institutions. The Eleventh International Conference on Emerging Security Information, Systems and Technologies, 125–130. Retrieved from file:///C:/Users/Dell/AppData/Local/Temp/securware_2017_7_30_30093.pdf.

Wagiu, E. B., Siregar, R., & Maulany, R. (2019). Information System Security Risk Management Analysis in Universities Using Octave Allegro Method. Abstract Proceedings International Scholars Conference, 7(1), 1741–1750. https://doi.org/https://doi.org/10.35974/isc.v7i1.1387.

Wangen, G., & Snekkenes, E. (2013). A Taxonomy of Challenges in Information Security Risk Management. NISlab Norwegian Information Security Laboratory. Retrieved from https://www.researchgate.net/publication/318853192_A_Taxonomy_of_Challenges_in_Information_Security_Risk_Management.

Wang, C., & Chen, D. (2023). Assessing Cybersecurity Risks in Higher Education: A Framework for Information Security Risk Management. Computers & Education, 30(1), 125-140.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). ScienceDirect A situation awareness model for information security risk management. Computers & Security, 1–15. https://doi.org/10.1016/j.cose.2014.04.005.

Yilmaz, R., & Yalman, Y. (2016). A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. Tem Journal, 5(2), 180–191. https://doi.org/10.18421/TEM52-10.

Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. Risk Management and Healthcare Policy, 9, 75–85. https://doi.org/10.2147/RMHP.S99908