International Journal of Advanced Research
ijar.eanso.org
Volume 6, Issue 1, 2023
Print ISSN: 2707-7802 | Online ISSN: 2707-7810
Title DOI: https://doi.org/10.37284/2707-7810

EASO
EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

The Institutionalisation of Information Security Management Practices in selected Organisations in Uganda

Benjamin K. Ahimbisibwe[1*] & *Peter Nabende*[1]

[1] Makerere University P. O. Box 7062, Kampala, Uganda.
* Author for Correspondence ORCID ID: https://orcid.org/0000-0002-0570-1274; Email: benja.kasiisi@gmail.com.

Article DOI: https://doi.org/10.37284/ijar.6.1.1155

Publication Date:

30 March 2023

Keywords:

Information Security, Information Security Governance, Information Security Management Practices, Institutionalization, Securing Information.

ABSTRACT

The study aimed at examining the extent to which information security management practices were institutionalised in corporate organisations. Evidence shows that failure by organisations to entrench the information security management practices (ISMPs) into organisations' structures opens the gateway for attacks, threat actors and information breaches to cause harm to information assets with ease. The study explored the phenomenon in its social setting hence the adoption of descriptive research design as the research methodology. The institutional theory was adopted as a new dimension in examining information security management in organisations. This theory suggests that control gears like coercive, normative, mimetic and management commitment could be used to effectively entrench security guidelines in organisations. Methodical scrutiny of the institutionalisation process: development, implementation and maintenance, and evaluation were also carried out. The researcher relied on human experience to make sense of the institutionalised processes. Extant literature was reviewed, and survey questionnaires were developed based on the eleven ISMPs and administered to purposively selected respondents from the two organisations. The eleven ISMPs covered include state of information security policy, asset management, secure information sharing, supply chain security, access management, network security controls, portable and removable media security, remote access security, protective monitoring of information systems, implementation of information security back-ups, and security accreditation by professional bodies. Data analysis was done using SPSS. Findings indicate that organisations have not fully incorporated all the eleven ISMPs covered as best practices and standards. Based on the results from the field, answers to the research questions were partly realised. Recommendations like the implementation of ISMPs to check deficiencies identified, customisation of security guidelines to protect information assets and institutionalisation of security practices at all levels were suggested.

This work is licensed under a Creative Commons Attribution 4.0 International License

Overall, the study was a positive step towards the institutionalisation process of ISMPs in organisations.

APA CITATION

Ahimbisibwe, B. K. & Nabende, P. (2023). The Institutionalisation of Information Security Management Practices in selected Organisations in Uganda *International Journal of Advanced Research*, *6*(1), 48-63. https://doi.org/10.37284/ijar.6.1.1155

CHICAGO CITATION

Ahimbisibwe, Benjamin K. and Peter Nabende. 2023. "The Institutionalisation of Information Security Management Practices in selected Organisations in Uganda". *International Journal of Advanced Research* 6 (1), 48-63. https://doi.org/10.37284/ijar.6.1.1155.

HARVARD CITATION

Ahimbisibwe, B. K. & Nabende, P. (2023) "The Institutionalisation of Information Security Management Practices in selected Organisations in Uganda". *International Journal of Advanced Research*, 6(1), pp. 48-63. doi: 10.37284/ijar.6.1.1155.

IEEE CITATION

B. K., Ahimbisibwe, & P. Nabende, "The Institutionalisation of Information Security Management Practices in selected Organisations in Uganda", *IJAR*, vol. 6, no. 1, pp. 48-63, Mar. 2023.

MLA CITATION

Ahimbisibwe, Benjamin K. & Peter Nabende. "The Institutionalisation of Information Security Management Practices in selected Organisations in Uganda". *International Journal of Advanced Research*, Vol. 6, no. 1, Mar. 2023, pp. 48-63, doi:10.37284/ijar.6.1.1155.

INTRODUCTION

Information Security Management Practices (ISMPs) in organisations have become one of the major concerns as evidenced by some studies (Whitman and Mattord, 2014; Alshaikh *et al.*, 2014; Carcary *et al.*, 2016; Maynard *et al.*, 2018; Schinag and Shahim, 2020; Culot *et al.*, 2021; Ahimbisibwe and Nabende 2022; Herath *et al.*, 2022). Findings from these studies demonstrate that not all organisations implement the recommendations suggested. Therefore, failure to incorporate security management practices is a concern to almost all organisations irrespective of size, objective, nature, or location. This is a fact undisputable almost by all stakeholders in existing organisations. According to Abercrombie *et al.* (1988), institutionalisation is a process by which social practices are continuously repeated, sanctioned and maintained by social norms to acceptable levels within the organisation structure. This process (institutionalisation) recognises changes or practices adapted to incorporate new perspectives involved in the implementation process (Wals, 2014). In the context of this study, the process relates to the identification of basic conflicts between regular organisational practices and standard fixed practices. Any organisation interested in securing information assets should adapt to changes, prepare to incur expenses in terms of money, time and commitment towards sustainability and operationalisation of the appropriate practices (Culot *et al.*, 2021). Exploring this argument helped to contextualise this study. The study set out to establish the extent to which ISMPs are institutionalised in selected organisations in Uganda. The researchers used Kabale University (KAB) and Bishop Barham University College (BBUC) as case studies. Our line of thinking was to find out the controls used, their importance and the degree of operationalisation in these organisations. This paper is anchored on the following research question: *to what extent are the information security management practices institutionalised in corporate organisations in Uganda?*

According to the current study, eleven information security management practices were covered. These include the state of information security policy, asset management, secure information sharing, supply chain security, access management, network security controls, portable and removable media security, remote access security, protective monitoring of information systems, implementation of information security back-ups, and security accreditation by professional bodies (Ahimbisibwe and Nabende, 2022). A critical examination of these practices reveals that there was a need to fill the knowledge gap exposed by investigating the real situation in the selected organisations, hence the need for the study. Broadly, the study found that none of the selected organisations could balance the implementation of ISMPs (technological and managerial), as will be discoursed in the literature review of this paper. The literature review section will cover categories of ISMPs, factors affecting I.S.M. success, information security institutionalisation process, and institutionalisation of information security management practices in Uganda. The third section explains the methodology adopted, followed by the presentation of findings in section four. The fifth section presents the discussion of results, conclusion, recommendations and opportunities for further research. It is apparent and rational to understand the institutionalisation of ISMPs in organisations given the importance allotted to information as a major asset in achieving set objectives; hence the purpose of this paper was to assess the extent to which ISMPs were entrenched in selected organisations in order to recommend suitable recommendations to operationalise the practices.

LITERATURE REVIEW

Existing literature show that most organisations have tried the implementation of technical information security practices (Whitman and Mattord, 2014; Alshaikh *et al.*, 2014; Carcary *et al.*, 2016; Maynard *et al.*, 2018). Whereas literature (see *Table 1*) shows that organisations have tried to implement technical security practices like proper configuration of firewalls, locking down servers, implementation of intrusion detection services, cryptographic solutions, network security etc., available studies have equally demonstrated that less attention has been given to managerial information security practices such as the implementation of policy, awareness and training, compliance with security standards, etc. (Alshaikh, 2016; Ahimbisibwe and Nabende, 2022; Herath *et al.*, 2022).

Table 1: Studies on information security management practices in organisations

Authors	Context	Methodology	Key findings
Doughty (2003)	Information security in a medium size organisation	Gap analysis	Implementation of an enterprise security framework is a must and rewarding
Khalfan (2004)	I.T. outsourcing projects of public and private sector organisations in Kuwait	Questionnaire survey and semi-structured interviews	Information security risks outdo other project outsourcing concerns like loss of control
Zakaria (2004)	Information Security culture challenges in a public sector organisation in Malaysia	Questionnaire, interviews, and document review	Identification of employees' information security behaviour
Harnesk and Lindström (2011)	Analysing security conduct in public nursing centres	Interviews	Discipline and agility play a vital role in security
Singh *et al.* (2013)	I.S.M. practices of Indian and German organisations	Semi-structured interviews	Industry type, organisation size and culture and regulatory

Authors	Context	Methodology	Key findings
			compliance are key determinants of ISM
Parsons *et al.* (2014)	Information security vulnerabilities in 3 Australian government organisations	Web-based questionnaire	Key information security awareness concerns include wireless security, social media and reporting of sec incidents
Singh and Gupta (2019)	ISM practices of organisations from India	Semi-structured interviews	Identification of linkages among various ISM factors to explore causal relationships among each other

Categories of Information Security Management Practices

Information security management practices are standards or sets of guidelines systematically designed to manage an organisation's information assets. According to Alshaikh *et al.* (2014), the term information security management practice (ISMP) refers to the individual management-level activities that organisations can implement to achieve information security objectives. For this to be achieved, the industry standards in the area of information security (e.g., ISO 27000 series) advocate that organisations need to select appropriate managerial and technical security controls in order to achieve their information security objectives. However, reviewed literature show that the practices provided by ISO 27000 standards do not provide a distinction between managerial and technical activities (Alshaikh *et al.,* 2014). Despite this, ISO 27000 standards (Disterer, 2013) provide a list of management practices towards achieving organisational security objectives.

These eleven security practices form the domains covered in this study which include security policy, organisation of information security, asset management, human resources security, physical and environmental security, communication and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management, and compliance. They are designed to minimise risk and ensure business continuity by proactively limiting the impact of security breaches. A detailed description will be covered in sections four and five.

Factors affecting Information Security Management Success

This study identified the key factors affecting information security management success from the practitioners' perspective as suggested by Zammani and Razali (2016). According to these authors, the following are the factors affecting information security management success as shown in *Table 2*.

Table 2: Information security management success factors and elements

Aspect	Factors	Description
A: People		These are individuals or teams directly involved in the planning, implementation, evaluation and improvement of ISM processes.
1.	Top Management	Knowledgeable in ISM governance, provide leadership and commitment, accountable, support, monitor and review ISM.
2.	ISM Team	Designated staff involved in most information security activities, skilled, knowledgeable, and committed to the assigned tasks.
3.	Coordinator Team	Coordinate ISM activities, manage major ISM documents and activities, and liaise with top management, ISM team, IS audit team and employees.
4.	IS Audit Team	The team accounts for all IS controls, processes, procedures, and activities. Members should possess appropriate knowledge of the people, processes, and procedures that need to be audited.
5.	Employees	The organisation's employees should have an awareness of the IS policy, controls, threats, and risks in order to comply with the IS policy, rules, and laws and reduce security incidents.
6.	Third Parties	These are individuals or companies involved in providing services to organisations on a contract basis at a particular time. Third parties should be aware of and comply with security policies, regulations and contracts.
B: Organisation		These aspects refer to the strategic and technical documents that are established and followed during the ISM processes.
7.	IS policy	IS policy is a strategic document that consists of objectives, directions and rules that must be established and followed by all stakeholders (entire employees and third parties).
8.	IS procedures	These are operating guidelines that contain a series of actions that explain how to perform IS processes. They are directly derived from the IS policy.
C: Process		The main processes involved in ISM include resource planning, competency development and awareness, risk management, IS auditing and business continuity management.
9.	Resource planning	This is essential to support and perform ISM processes. Resource planning consists of financial resources and human resources. Financial resources comprise the cost of buying new assets, maintaining existing assets, manpower costs and the cost of performing IS activities. Human resources include the teams or individuals to be engaged in ISM activities.
10.	Competency development and awareness	This can be gained through training and awareness programs. Training programs help people to acquire knowledge and skills in task handling. Awareness programs are designed to ensure that people are aware of IS policy, threats, and risks as well as their roles and responsibilities.
11.	Risk management	Risk management is a process of measuring and analysing risk levels and taking appropriate actions to control them. The process comprises risk assessment and risk treatment. Sub-activities such as establishing the risk acceptance criteria, identifying assets and threats, determining the impacts and probability of risk incidents, and determining the risk levels from risk

Aspect	Factors	Description
		assessment, while risk treatment involves the activity of implementing the protection strategies based on the risk assessment results.
12.	IS Audit	The components of the audit process include an audit program which consists of audit planning, audit execution, and auditor training; audit findings and reporting; follow-up audit to check the corrective and preventive actions that have been done
13.	Business Continuity Management	Business continuity management ensures the organisation's businesses operate smoothly during and after unintended events. When unintended events occur, a business continuity plan that outlines the resources, processes, procedures, and responsibilities should be activated. Organisations shall carry out periodic tests on the business continuity plan to ensure its validity and effectiveness.

Source: Zammani and Razali (2016)

Information Security Institutionalization Process

The institutionalisation process, as explained by Crossan and Bedrow (2003), involves deliberate efforts aimed at entrenching routine actions in organisation structures at all levels. In this study, the process involved embedding ISMPs to regulate organisational information assets. The institutionalisation process is treated as a building block comprising three phases, i.e., development, implementation and maintenance, and evaluation. These phases serve as a foundation plan to mitigate challenges in the institutionalisation processes.

Development phase: There is a need for organisations to develop appropriate controls based on the established security policy and philosophy so that employees and stakeholders can be mindful of possible threats to information or critical infrastructure and adopt appropriate actions to mitigate them. During this phase, all the characteristics of likely threats, threat actors, and stakeholders, including information classification and the appropriate security actions are considered (Mbowe1 *et al.*, 2014).

Implementation and maintenance phase: This is the second phase aimed at ensuring that appropriate information security controls become operational. The process allows employees and stakeholders to get training on the implemented information security mechanisms. Once the ISMPs have been executed, then organisations enter into the maintenance sub-phase.

Evaluation phase: The third phase is *evaluation***.** During this phase, management is prompted to conduct a review of the implemented ISMPs by identifying new security challenges, threats and aligning them to newly developed security controls.

Institutionalisation of Information Security Management Practices in Uganda

Uganda like most developing countries has made some noticeable progress in the operationalisation of ISMPs in various organisations (Alshaikh *et al.*, 2014). This was evidenced through the implementation of some measures in a phased mode like policies, asset classification, controls, monitoring, restrictions, authorisation rights and identification by management which have positively impacted information security in organisations. Therefore, justification for the need to protect organisational information assets (Luesebrink, 2011). The study focused on the degree to which ISMPs are operationalised in selected organisations in Uganda, particularly Kabale University (KAB) and Bishop Barham

University College (BBUC). These two organisations were chosen based on ownership and control. Whereas KAB is a public university owned, controlled and funded by the government of Uganda, BBUC is owned and managed as a private university. Despite the nature of their ownership or management, both organisations provide services in the education sector and have exhibited some level of operationalisation of information security management practices as presented in section five (findings).

Scholars like Rehman *et al.* (2013) assert that partial implementation of security measures is done by a skeletal technical group that is controlled by the Information Technology department. This skeletal staff find it impossible to fully operationalise the information security measures, monitor activities of wrong elements or detect threat attacks. Such is the status of the two selected organisations. Although evidence suggests that to a less extent, KAB and BBUC have adopted security measures such as risk assessment, security plan, adopting best practices, and identifying threats and vulnerabilities to counter the likely breaches, much needs to be done. There are still gaps in the implementation process that require management's attention. The security measures are not fully implemented due to limited budget allocations and support from top management. From the findings, there was still a challenge of convincing top management to fully accept the responsibility or be fully accountable for the actions regarding the security of information assets in the two organisations. Details of the current state could easily be depicted from the findings presented in section five and discussed in section six of this paper.

METHODOLOGY

The study adopted a descriptive research design using a qualitative approach. A population of 60 respondents of which 30 were from KAB and 30 from BBUC were targeted. This population comprised the University Secretary, Academic Registrar, Faculty Administrators, Director of ICT, System Administrators, IT Officers, E-learning Officers, Examination Officers, Records Officers, Office Secretaries and Security Officers. Questionnaires were preferred as data collection tools to obtain raw data from the participants because of being logically structured, reliable and cost-effective. An exploratory case study was initially conducted with the aim of identifying ISMPs at the Uganda Wildlife Authority (UWA) and National Forest Authority (NFA), both public institutions. Data collection tools used were later refined to conduct the present study at KAB and BBUC. The data collected were coded into a computer system and analysed using the Statistical Package for Social Scientists (SPSS), where percentage distributions were generated according to the respondent's profile. Using the selected organisations, a structured analysis of practices critical to information security assets management was made, and the factors affecting information security management success and the degree to which information security management practices were operationalised were established. The researchers also reviewed related literature by focusing on key areas pertaining to the institutionalisation of information security management practices to back up the methodology.

RESULTS

In this section, data on the extent to which information management practices were institutionalised in the two organisations were presented. The results were presented by showing percentages depicting respondents' views and later discussed in section six to give the reader a segmented flow of argument. These results cover the eleven information security management practices as summarised in the subsequent sub-themes as follows:

Article DOI: https://doi.org/10.37284/ijar.6.1.1155

State of Information Security Policy in the Organisations

The questions under this practice were to probe the state of information security policy in the selected organisations. It was established 84% of the respondents that the policy does not define the purpose, scope, and approach to managing information security within the organisation and 82% noted the policy does not apply to all the activities linked to protecting information security systems. It was also noted that (76%) policy does not explain how the organisation and supply chain protect information and physical assets; (72%) was not publicised and made readily available to all staff. 70% of the respondents further noted that the policy does not undergo regular review to ensure its continuing relevance; (64%) policy does not specify penalties for breaching the policy and related security measures. Management has not drafted, obtained university council approval and published an information security policy that addresses the National Information Security Policy mandatory minimum requirements in terms of the organisation’s business requirements, threat environment and risk appetite (40%) as well as (36%) policy does not specify a review cycle in order to ensure its continued applicability. Similarly, 36% of the respondents claimed the policy doesn’t know organisations specify a review cycle in order to ensure its continued applicability; 40% noted the policy does not know defined acceptance and compliance arrangements by staff and the supply chain.

Asset Management Requirements

By examining the information security asset management requirements practice, findings indicated that management (100%) does not use approved criteria to create a definitive register of business-critical facilities, systems, sites, and networks; (76%) management does not designate a suitably empowered owner for every asset. It was noted by 60% of the respondents that the management does not ensure that designated divisions own and secure named information assets; 60% claimed the management does not label and handle information assets throughout their lifecycle in accordance with Security Standard No. 3 – Security Classification (SS3). In addition, 60% reported the management to have an inventory of their assets drawing up and maintaining a register of important assets as a prerequisite to risk management; (64%) management have to inform the Board of the main security risks affecting vital business assets. 64% of the respondents noted that management has to identify, document and enforce rules of acceptable use of information assets and 76% of the respondents pointed out the organisation have to audit the asset register regularly. 76% reported that the organisations have to use the Government Security Classification Standard to determine the acceptable procedures for labelling, handling, transmitting and decommissioning assets, while 100% pointed out that management has to ensure that assets associated with critical infrastructure receive the level of protection appropriate to their value, sensitivity and criticality.

Secure Information Sharing

From the findings, it came out that (100%) management does not require internal and external entities to show compliance with mandated national information security requirements and approved security policies before sharing or allowing connections to protected computer assets; (100%) management does not create information exchange policies and procedures; All the respondents (100%) reported that management does not assess compliance of exchange partners at least annually or when required; (100%) management does not ensure that users are fully conversant and comply with approved information exchange policies, procedures, controls and relevant national legislation. However, 76% of the respondents noted that management does not confirm that receiving parties grasp and are complying with their obligations to protect information assets appropriately, while 60% pointed out that all users including board members, senior executives, employees, and third-party users – do not obtain security awareness before gaining access to critical infrastructure. Management does not adopt policies to handle information assets received from foreign countries and international bodies in line with applicable treaties and arrangements (60%) as well as does not know organisation disconnect/end share with non-compliant entities (40%). 40% of the respondents reported that they don't know organisations use formal exchange agreements such as codes of connection and memoranda of understanding, while 76% don't know management ascertains that exchange agreements with external parties are enforceable. In addition, 76% noted that management has to identify and record risks involving external parties, while 40% claimed management has to obtain authorisation before granting third parties access to information and ICT systems owned by another organisation.

Supply Chain Security

The results show that management (100%) does not establish consistent supply chain security processes with clear lines of accountability. All the respondents pointed out that (100%) management does not abide by PPDA instructions to identify, document and incorporate security requirements into outsourcing contracts with suppliers and contractors. Management does not require contractors to present an operational security management plan outlining their strategy for reducing security risks to acceptable levels (100%). 76% noted that management does not ensure that the computer networks, products and services supplied do not introduce information security risks; 76% believed that management does not recognise that they retain accountability for managing their information risks even where they outsource ICT systems and services to third parties. Also, 76% of the respondents claimed that management does not ensure that they are fully acquainted and compliant with the national security impact assessment process for ICT suppliers, while 64% believed that management does not at least annually, obtain independent assurance that suppliers are complying with the mandated NISF requirements and other security policies.

About 60% of the respondents noted that management does not outline the process for the development and maintenance of procedures, processes, instructions and plans for securing the system, while another 60% noted that organisations have to mitigate risks of intentional and unintentional supply chain compromise. Management does not issue Security Aspects Letters (SAL) regularly to update contractors on the security conditions that govern their access to critical infrastructure assets (40%) as well as 40% don't know management identifies and evaluates the security risks related to outsourcing or offshoring before letting contracts for critical infrastructure and services. Consequently, 40% of the respondents don't know management includes security clauses in service contracts; 40% don't know organisations ensure that suppliers are subject to and pass a national security impact assessment. 76% believed the management has to assess compliance with requirements at least annually, and 76% also noted management has to enforce sanctions for non-compliance.

Access Management

The respondents (80%) indicated that management has to harden and lock down user applications such as web browsers and office productivity applications to reduce exposure to software vulnerabilities. 76% noted the management has to enable regular review of access rights, while 64% claimed management has to require appropriate identification and authentication techniques for all IT systems. About 64% of the respondents reported that management has to enable organisations to deter, detect, resist and defend against accidental or deliberate unauthorised actions, while 64% claimed the management has to ensure that only users,

Article DOI: https://doi.org/10.37284/ijar.6.1.1155

processes and devices with a business need to know and suitable security clearances gain access to critical infrastructure.

The respondents (60%) indicated that the management has to define and document business requirements for access control and restrict access to critical infrastructure to those who satisfy these requirements as well as 60% noted that the management has in place a formal process for user password management. 60% reported that the management does not adopt an access control policy that enforces the principle of least privilege, while 64% affirmed that the management does not ensure that users are aware of and abide by their responsibilities to maintain access controls such as passwords. 40% don’t know management uses formal access registration and revocation processes, while all the respondents claimed (100%) management does not enforce recommendations of access rights reviews, e.g. disable user. All the respondents also (100%) noted that management does not follow a formal access control policy linked to HR processes.

Network Security Controls

The data gathered on network security controls indicate that (100%) management has not adopted the defence-in-depth principle in the organisation; (100%) management does not adopt solutions that use techniques such as encryption to offer converged voice, data and video packet protection appropriate to their security needs. All the respondents (100%) indicated that the management does not ensure that users only gain access to network services, e.g., web browsing and file upload, if they have a legitimate business reason for the access. 76% noted that the organisation does not segregate networks handling information of different business impact levels. In addition, 76% noted that the organisation had not adopted the “defence-in-depth” or “layered” approach to network security through the use of different technical security controls and security products to mitigate security threats collectively.

The data gathered on network security controls further indicate that (64%) of organisation do not apply technical security controls appropriate to the protected computer’s value, sensitivity and criticality. 60% of the respondents reported the management does not enforce sufficient segregation, zoning or variable depth security to separate specific areas of the network, groups of information services and information systems handling data of different security classification levels. In addition, 60% claimed the organisation do not implement boundary protection measures for shared networks, especially those extending across organisational boundaries, in compliance with the access control policy and requirements of the business applications; (60%) management does not enforce network routing controls to ensure that connections and information flows do not breach the access control policy of the business applications; 60%) organisation do not use unified authentication, and authorisation services; (60%) organisation do apply the principle of service minimisation consistently across the network by disabling services that do not satisfy business and security needs for access.

The respondents (40%) further indicated that organisations do not install network intrusion detection (NIDS) and network intrusion protection (NIPS) devices to monitor network traffic for unusual or suspicious activity and prevent cyber-attacks. 60% reported that organisations do build survivability into networks to ensure that technical solutions continue to deliver a minimum set of essential functionalities in a timely manner, even if parts of the network are unreachable or have failed due to an attack. 76% affirmed the organisation do adopt a security architecture that provides end-to-end network security by enabling the detection, identification and correction of security vulnerabilities. Another 76% believed the organisation have a formally documented security architecture providing end-to-end network security, while 40% noted not know whether the organisation matched security levels with information protection needs.

Portable and Removable Media Security

It was established that (76%) of management does not prevent the holding, storage and processing of sensitive information on personal devices. 74% of the respondents indicated the management does not conduct user awareness training audits and user actions. 40% of the respondents claimed management does not perform a formal risk/benefit analysis before the use of the removable media, while 60% established the management has a formal policy that requires authorisation to use and transfer the media. 40% believed the organisation does not encrypt devices to deter unauthorised access; however, 60% noted that the management had enforced a security policy on media to detect and resist unauthorised use. 64% of the respondents indicated the management has a baseline, by default, lockdown access to media drives. 64% reported the management to have a user of portable and removable media adopted formal procedures to prevent the unauthorised disclosure, modification, removal or destruction of assets and interruption to business activities.

Remote Access Security

It is evidenced from the findings 100% of the respondents affirmed that organisations had not adopted a formal remote access policy, while 80% reported management does not educate users about remote access risks. 78% noted the management does not have security accredited remote access solution handling classified data. 76% pointed out the management does not use security controls like encryption to protect data whilst at rest and in transit. 74% affirmed that the management does not implement appropriate security measures to mitigate remote access risks, while another 74% reported management does not align remote access policy with incident management plans. 64% of the respondents also noted that management has to assess the risks, threats and vulnerabilities of remote access.

Protective Monitoring

A look at the respondents’ views shows that (84%) organisation have not established procedures for reviewing monitoring results. 82% believed the organisation does not define and adopt a protective monitoring strategy that defines the objectives, approaches and resources required to support consistent organisation-wide accounting, audit and monitoring activities. 76% affirmed that the organisation does not implement measures to detect and tie to users’ unauthorised information processing activities. 72% reported the organisation does not protect audit logging facilities and log data, while 70% pointed out the organisation does not produce and preserve, for an agreed time, audit logs recording user activities, exceptions, faults and security events. 64% claimed the organisation does not train staff to interpret monitoring results. However, 36% noted that the management had aligned protective monitoring with incident management and HR policies, while 40% didn’t know organisations have in place an accounting and audit policy that complies with business requirements for real-time security accounting and audit.

Information Back-Ups

Findings indicate that all the respondents (100%) reported that the organisations do not define the required backup levels; 80% of the respondents claimed that the organisations do not store backup data a safe distance away from the main site. 78% noted that the organisations do not afford backup information suitable for physical and environmental protection, while 76% reported the organisations do not produce accurate and complete records of backup copies. 74% affirmed that the organisations do not adopt formal policies and procedures to back

Article DOI: https://doi.org/10.37284/ijar.6.1.1155

up and regularly test copies of information and software required to recover from major disruptions. The respondents 74%) indicated that organisations do not test backup media regularly to ensure its recoverability, while 64% pointed out that organisations have based the frequency of back-ups on the value, criticality and sensitivity of data.

Security Accreditation by professional bodies

According to the results from the field, 84% of the respondents affirmed that the management does not accept and retain accountability for accreditation. 84% claimed the management does not have accreditation plans, while 74% pointed out that the management has not developed an accreditation roadmap. 70% of the respondents reported that management does not define an accreditation boundary; (64%) management has to ensure that every IT project has a senior responsible owner; (38%) all computers in the organisation are not accredited to the national information security policy risk management and accreditation standard. Similarly, 38% don't know whether all computers in the organisation are accredited to the national information security policy risk management and accreditation standard.

DISCUSSION

A total of 50(83%) respondents returned the questionnaires answered, with 37(74%) representing KAB while13(26%) represented BBUC. In general, 83% responded to the questions that covered the eleven ISMPs investigated, which shows a very good response. According to the results presented in section five, the majority of the respondents were not aware of the state of information security policy in both organisations. This meant that even if the document existed, stakeholders in these organisations could not follow the rules established or guidelines specified due to a lack of awareness. An information security policy is mandated to improve the security of information in organisations (Zammani and Razali, 2016). This objective can only be achieved if the policy is institutionalised. Institutionalising the policy entails publishing, enforcing and regularly updating the document to reflect organisational requirements (NITA, 2014). This process requires organisations to follow approved criteria to create a definitive register, well labelled, registered and regularly audited showing critical business facilities, systems, sites and networks under the responsibility of a designated person authorised as the asset owner.

Results from the field show that management does not require to secure information being shared with internal and external entities and shows compliance with approved security policies before sharing information or connecting to protected computer equipment. This implies that there is no need to establish information exchange policies, procedures, controls and regulations. Such a condition is disastrous to information and needs a solution, which is the institutionalisation of ISMPs (D'Arcy *et al.*, 2014). The researcher agrees with suggestions advanced by D'Arcy *et al.* (2014) which targeted understanding stressful information security situations. This demands security measures that involve the institutionalisation process to identify and record all risks associated with external parties including information exchange policies, procedures, formal exchange agreements, memoranda of understanding and periodic assessments of compliance between entities. A similar situation also applies to circumstances that concern the supply chain. Organisations need to establish consistent supply chain security processes with clear lines of accountability, compelling suppliers to national security validation and signing service contracts designed to enforce sanctions against non-compliance.

According to the results presented in section five, the majority revealed that organisations need to institutionalise access management practices in order to ensure authorised users, processes, and devices gain access to infrastructure. This necessitates establishing and implementing a formal

Article DOI: https://doi.org/10.37284/ijar.6.1.1155

access control policy linked to human resource processes (Peltier, 2016). Using formal access registration, revocation process, appropriate identification, authentication techniques, and resistance against unauthorised actions can be conducted to review access rights. The same process would apply to network security controls to help organisations institute appropriate risk-based technical security measures for portable and removable media, remote access, and secure backup systems. As a minimum requirement, organisations require the adoption of the defence-in-depth principle providing end-to-end network security and specified enforcement actions against wrongdoers. This call for organisations to invest in conducting user awareness training (Stallings *et al.*, 2012), auditing user actions, preventing the processing of sensitive information on personal devices, establishing remote access policy aligned with incident management plans, storage backup data establishing a safe distance away from the main site tested for recoverability.

Furthermore, analysis of the results shows that the evolution of ISMPs in organisations provides a clear plan to provide stakeholders with relevant information on how an organisation complies with minimum security (Ashish *et al.*, 2021). This would demonstrate compliance with security requirements as stipulated by a professional body accredited to secure information outlining standard guidelines, procedures, processes, instructions and plans designed to maintain the security of information throughout its lifecycle. To achieve this mandate, organisations should identify and address major risks to vital systems (Walid and Mohammad, 2013). This would require organisations to accept and retain accountability for accreditation, ensure that every information asset has a responsible owner, and define an accreditation boundary, roadmap and plan for securing the system.

CONCLUSION

This study generally dealt with the degree to which ISMPs were institutionalised in the two selected organisations in Uganda. Overall, results indicated that ISMPs were not fully implemented as anticipated. The selected organisations, i.e. KAB and BBUC did not have a well-put-down policy statement on information security, lacked clear and effective structures for managing information security, and lacked adequate information security, awareness and training for the users and stakeholders. This makes it easy for attackers to compromise the security of information in organisations. Besides, these organisations did not have in place well-streamlined business continuity and disaster recovery plans nor adequate information risk incident mechanisms. Besides, the partially implemented ISMPs did not have in place streamlined business continuity and disaster recovery mechanisms nor adequate information risk incident mechanisms.

One major challenge, though was that some users were non-compliant with set information security guidelines. The fact that these organisations lacked adequate information asset management measures, information shared was not fully secured, the supply chain for information systems was not secured, information could be accessed by unauthorised persons, no restrictions for the use of portable storage media, and lacked adequate protective monitoring mechanisms for information backups. As established, the study provides rich insight into the institutionalisation of ISMPs in organisations. It also offers answers to the research question advanced by recommending acceptable security measures designed to improve the effectiveness of information security management in organisations, as highlighted in the discussion section. It should be acknowledged that this is a positive step towards the ISMPs institutionalisation process that may lead to their thorough operationalisation in organisations.

Recommendations

Based on the discussion of findings, the following were strongly recommended as requirements for institutionalising information security management practices in organisations.

Table 3: Recommended requirements for institutionalising information security management practices

Requirement	Category
Appropriate information security policy	Managerial
Established asset management criteria	Technical and managerial
Secure information-sharing controls	Technical and managerial
Established supply chain security process	Technical and managerial
Access management services	Technical and managerial
Network security controls	Technical
Secure portable and removable media devices	Technical and managerial
Remote access security policy	Technical and managerial
Protective information systems monitoring approach	Technical and managerial
Implementation of an information security back-ups plan	Technical and managerial
Establish a security accreditation body	Professional

Source: Researcher, 2022

As observed in *Table 3* above, organisations were recommended to institutionalise managerially a mixture of both technical and managerial security controls, purely technical or professional security controls depending on the activities practiced and the objective to be achieved. The study further recommends that total institutionalisation would necessitate support from top management, implementation of established information security policies and measures and working with an established professional security accreditation body mandated to ensure quality and compliance as per the reputable procedures, processes and instructions, among other measures.

Areas For Further Research

The current study focused on academic institutions. There is a need to conduct a similar study in other organisations like private profit-making institutions (e.g., financial organisations) in order to cross-validate the findings.

ACKNOWLEDGEMENTS

This work could not have been possible without the financial assistance and moral support, especially prayers rendered by my family, chiefly my wife Ms. Katabarwa Grace. Secondly, I wish to thank my Supervisor, Dr. Nabende Peter for his invaluable input and support throughout the research process. Finally, we would like to extend our sincere thanks to the organisations and all participants in the study for their time, experiences and willingness to engage in our research up to successful completion.

REFERENCES

Abercrombie, N., Hill, S, & Turner, B. (1988). *Dictionary of Sociology*. Second edition. Penguin.

Ahimbisibwe, B., & Nabende, P. (2022). A conceptual framework for assessing information security management practices in selected universities in Uganda. *Journal of Digital Science*.

Article DOI: https://doi.org/10.37284/ijar.6.1.1155

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). Towards a taxonomy of information security management practices in organisations. ACIS.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2016, July). Information security management practices in organisations. In *4TH Annual Doctoral Colloquium* (p. 52).

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report*, 13(4), 195–201

Ashish, U., Mantha, S., & Reddy, N. (2021). Analysis of evolution of information security

management practices in organisations providing IT development & IT Enabled services, *International Journal of Engineering Research and Applications.* ISSN: 2248-9622, Vol. 11, Issue 5, (Series-VI) May 2021, pp. 18-24

Bjorck, F. J. (2004). Institutional theory: a new perspective for research into IS/IT security in organisations. System Sciences Proceedings of the 37th Hawaii International Conference on, IEEE Computer Society Press http://ieeexplore.ieee.org/servlet/opac?punumber=8934

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for information security governance and management. *It Professional*, *18*(2), 22-30.

Crossan, M., & Bedrow, I. (2003). Organisational learning and strategic renewal. *Strategic Management Journal*, 24, 1087-1105.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of management information systems*, *31*(2), 285-318.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2).

Doughty, K. (2003). Implementing enterprise security: A case study. *Computers & Security*, 22(2), 99–114.

Harnesk, D., & Lindström, J. (2011). Shaping security behaviour through discipline and agility: Implications for information security management. *Information Management & Computer Security*.

Herath, T.C., Herath, H.S.B. & Cullum, D. (2022). An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks. *Inf Syst Front* (2022). https://doi.org/10.1007/s10796-022-10246-9

Mbowe1, J. E., Zlotnikova1, I., Simon, S. M., & George, S. O. (2014). A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy.

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: A descriptive case study of two sectors. *International Journal of Information Management*, 24(1), 29–42.

Luesebrink, M. (2011). Institutionalisation of Information Security Governance Structures in Academic Institutions: A Case Study.

Maynard, S., Tan, T., Ahmad, A., & Ruighaver, T. (2018). Towards a framework for strategic security context in information security

Article DOI: https://doi.org/10.37284/ijar.6.1.1155

governance. *Pacific Asia Journal of the Association for Information Systems*, 10(4), 4.

National Information Technology Authority (NITA) Uganda. (2014). National Information Security Framework (NISF) Publication National Information Security Policy.

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of management review*, *16*(1), 145-179.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC press.

Rehman, H., Masood, A., & Cheema, A. R. (2013). Information security management in academic institutes of Pakistan. In 2013 2nd National Conference on Information Assurance (NCIA) (pp. 47-51). IEEE.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? "From the basement to the boardroom": towards digital security governance. *Information & Computer Security*.

Singh, A. N., & Gupta, M. P. (2019). Information security management practices: case studies from India. *Global Business Review*, *20*(1), 253-271.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ism) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), 225-239.

Stallings, W., Brown, L., Bauer, M. D., & Howard, M. (2012). *Computer security: principles*

and practice (Vol. 3). Upper Saddle River: Pearson.

Walid, A. A., & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science*, *2*(2), 28-43.

Wals, A. E. (2014). Sustainability in higher education in the context of the UN DESD: a review of learning and institutionalisation processes. *Journal of Cleaner Production*, *62*, 8-15.

Whitman, M., & Mattord, H. J. (2014). Information security governance for the non-security business executive.

Williams, M. C. (1997). The institutions of security: elements of a theory of security organisations. *Cooperation and Conflict*, *32*(3), 287-307.

Zakaria, O. (2004). Understanding Challenges of Information Security Culture: A Methodological Issue. In *AISM* (pp. 83-93).

Zammani, M., & Razali, R. (2016). An empirical study of information security management success factors. *Commitment*, *5*, 7.