International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Ensuring Effective Information Security Management: Information Classification and Access Control Practices

Rosemary M. Shafack[1], Awiye Sharon Serkwem[2]

[1]Associate Professor, [2]PhD Student,
[1,2]University of Buea, Buea, South West Region, Cameroon

ABSTRACT

This study is based on information security management in financial institutions from the perspective of information classification and access control. As objectives, the study set out to assess information classification practices in microfinance institutions and their effect on overall information security management, and to examine access control in microfinance institutions and how it impacts information security management. The study made use of the Information Security Theory by Horne, Ahmad and Maynard, and a sequential exploratory mixed method survey research design. As data collection instruments, a questionnaire and an interview guide were used, with validity and reliability guaranteed by subject experts, ISO/IEC checklists, and Kuder Richardson formula 20 which realised a score of 0.81. Of the 30 managers and information security officers who participated in the study, a response rate of 100% was registered. To analyse data, descriptive statistics and thematic analysis were used. The findings portray loopholes in information classification and access control and thus in the information security management programme of participating institutions. Some recommendations put forth are; the need to adopt information classification schedules with distinguished levels of sensitivity, drafting of access control policies, signing of non-disclosure agreements and introduction of information security officers to ensure implementation and follow-up.

KEYWORDS: *Information Security, Management, Classification and Access Control*

How to cite this paper: Rosemary M. Shafack | Awiye Sharon Serkwem "Ensuring Effective Information Security Management: Information Classification and Access Control Practices" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.894-901, URL: www.ijtsrd.com/papers/ijtsrd38122.pdf

IJTSRD38122

INTRODUCTION

Internal and external threats to information have made it necessary for every organisation to secure data and information. According to Warkentin and Willison (2009), every organisation should protect their information from threats such as illegal access, unwanted interruption, unauthorised alteration and data annihilation. Because human beings (users) are the weakest link in the security chain (Sarkar, 2010; Warkentin & Willison, 2009; Hu, Xu, Dinev & Ling, 2011), issues related to access control must be taken seriously in the fight against information insecurity. This is because the risk associated to access especially in organisations that handle sensitive or confidential information, such as financial institutions is quite high. In fact, Zeneli and Düsterhöft (2016) emphasise that banks and financial institutions are the most vulnerable to information insecurity, and the financial industry records the highest costs per capita of information breaches and mismanagement. Since not all information is sensitive or of the same value, the risks associated to them differs too, and protection mechanisms should differ (Appleyard, 1998). Information must therefore be classified to ensure that it receives an appropriate level of protection in line with its importance (ISO/IEC, 2014b).

Statement of the Problem

In Cameroon, many financial institutions have over the years battled with securing information effectively. The researchers observed a trend over the last five years which is that of the continual recording of incidents which raise questions about account balances, identification and collateral documents have led many clients of such organisations to discontinue their services due to disappointments in how their information is managed. The researchers also noticed carelessness in the way staff handled information assets on their workstations, and how external storage devices like memory sticks were placed. Such acts could permit unauthorised users to access information illegally, and leave negative impact on the confidentiality, integrity and availability of information, and the organisation's finances, image, and reputation. Since information classification is an unavoidable necessity to determine access control for information, a study on information classification and access control practices in microfinance institutions in the Cameroon context was deemed necessary to bring to light the risks which information assets of such institutions are exposed to.

Objectives of the Study

The objectives of this study were to:

1. Assess information classification practices in microfinance institutions and their effect on overall information security management.
2. Examine access control in microfinance institutions and how it impacts on information security management.

Review of Literature

Information Security Management

Information Security Management is a series of management activities aimed at protecting and securing information assets within the framework of an organisation in which information system is running (Von Solms, 1998). In line with this, ISO/IEC 27000 (2014) explains that, management of information security is expressed through formation and use of information security policies, procedures and guidelines, applied throughout the organisation by all individuals associated with the organisation. Ashenden (2008), opines that, management of information security ensures the selection of adequate and proportionate security controls, and an unmanaged approach to information security makes it difficult for all risks to be adequately addressed. ISO/IEC 27001 (2005) connotes that a proper Information Security Management System (ISMS) includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources. To Tipton and Krause (2000), it is a set of coordinated activities to direct and control the preservation of confidentiality, integrity and availability of information (CIA).

Confidentiality has been defined as the property that information is not made available or disclosed to unauthorised individuals, entities, or processes (ISO/IEC 27000, 2014). Integrity is the property of accuracy and completeness of information (ISO/IEC 27000, 2014), to ensure that information remains original, complete, correct and trustworthy. Availability is the property of being accessible and usable upon demand by authorised entity (ISO/IEC 27000, 2014), and it ensures that information is made available and accessible to the right parties when need arises. Access control is one of the main counter measures to eliminate breach of confidentiality, integrity and availability of information.

Other properties of information which an ISMS must protect according to ISO/IEC are: Authenticity, which is the property that an entity is what it claims to be and guarantees the genuineness and correctness of information (ISO/IEC 27000, 2014); Accountability, which ascertains the responsibility of an entity (like a person) for its actions and decisions (ISO/IEC 27000, 2009) and ensures that actions and events can be traced to users, systems and processes that performed them; Non-repudiation, which is the ability to prove the occurrence of a claimed event or action and its originating entities (ISO/IEC 27000, 2014), and could help to resolve disputes about the occurrence or non-occurrence of an event or action and involvement of entities in the event (ISO/IEC 27000, 2009); and Reliability, which is the property of consistent intended behaviour and results (ISO/IEC 27000, 2014), and ensures that information is trustworthy, accurate and dependable.

The above-mentioned properties of information may be affected by natural and man-made factors and are the main reason why organisations protect information. Nosworthy (2000) explains that factors affecting information security management include; humans (to implement policies), organisational culture, attitudes of humans, security training, ownership and job description. Since human beings or the user is known to be the weakest link in the security chain (Gana, Abdulhamid & Ojeniyi, 2019), controlling access to information and information processing facilities is one of the most effective ways of ensuring security. Access cannot be fully controlled for all information assets if they are not classified.

Information Classification

Classification of information falls within Asset Classification in ISO/IEC 27002, and is the separation of information into classes according to classification scales or schemes. Using ISO/IEC 27001, there are four processes involved in managing classified information and these are: entering the information asset in the inventory, classifying the information into levels (such as confidential, restricted, internal use and public), information labelling and information handling (Kosutic, 2014). The essence of classifying information is to ensure that it receives an appropriate level of protection in accordance with its importance to the organisation (ISO/IEC, 2014b). In classifying information, the value, legal requirements, degrees of sensitivity and criticality need to be considered because some information assets might require an additional level of protection or special handling (ISO/IEC 27002, 2005). An information classification scheme is required to define protection levels and handling measures. Information classification, however, does not have many developed frameworks or guidelines (Oscarson & Karlsson, 2009), but classification by the system or guidelines is preferable over classification by the creator of the information (Al-Fedaghi, 2008).

Confidentiality, integrity and availability must always be considered when classifying information, in addition to access privileges and owner of the information (ISO/IEC, 2014b). In relation to confidentiality, Kosutic (2014) outlines four processes good for managing classified information, the first of which is entering the asset in the inventory**.** Inventory of assets helps the organisation to know which information is under her possession, different forms and types of media and who is responsible for it. The second process is classification of the information**.** At this stage, organisations can develop levels of classification based on their environment (industrial and national) since ISO/IEC does not prescribe these levels. Risk assessment is important in this process since information with higher value has higher consequences on confidentiality and thus requires higher classification levels. The number of levels of classification increase with the organisation's size. Kosutic presents the following levels which can apply for medium sized organisations: confidential (top confidential level), restricted (medium confidential level), internal use (lowest level of confidentiality) and public (everyone can see the information).

Information labelling is the next step and organisations must develop guidelines for each type of information asset and how to classify and label them. With paper documents for example, confidentiality level could be indicated in the top right corner of each page and on the cover or envelop (Kosutic, 2014). The last process is information or asset handling which is the most complicated stage in information classification and requires that rules for handling and protecting each type of information asset be developed according to the level of confidentiality. Kosutic exemplifies that; organisations can allocate 'internal use', 'restricted' and 'confidential' on the various levels. Some organisations

define procedures of information handling in their information classification policies. Bergström and Åhlfeldt (2014) explain that classified information can be dynamic, and change depending on the value of the information with time. Information has some attributes including sensitivity and level of analysis. Non-sensitive information can be unclassified and sensitive information classified, and the levels of classification are considered the basis for allocating access rights (Ahmad, Bosua & Scheepers, 2014).

Access Control

In selecting controls for information security management, management should include access control (Sattarova & Tao-hoon, 2007). This control enables organisations to manage how particular information resources, files, programmes and systems are accessed by different persons linked to the organisation. It necessitates the establishment and documentation of policies for information dissemination, authorisation, and access (ISO/IEC 27002, 2005). The main objective of access control is to restrict access to information. Sinclaire (2013) defines an access-control system as the set of mechanisms and processes employed to maintain the confidentiality, integrity, and availability of digital resources vis à vis the users who interact with them. Sinclaire found that access control as it is practiced is broken with symptoms like frequent over-entitlement, where a user has greater access than needed, and regular under-entitlement, where users are prevented from doing their jobs because they are unduly denied access.

Hu, Ferraiolo and Kuhn (2006) expressed that access control deals with determining and mediating allowed activities of legitimate users in the system, and the objectives are to protect system resources against inappropriate or undesired user access (optimal sharing of information). According to ISO/IEC 27002 (2005), user registration, privilege management, user password management, user access rights, user responsibility, use of password, non-negligence of equipment, clear desk and screen policy are encouraged. There is also network access control which is meant to prevent unauthorised access to internal and external networked services, authenticate users for external connections, identify equipment and ensure routine control of connections (ISO/IEC 27002, 2005). Log-on procedures are also encouraged in addition to mobile computing and teleworking aspects of access control aimed at ensuring information security when using mobile computing and teleworking facilities. Horne, Ahmad and Maynard (2016) bring out a clear explanation of information assets, threats, classification, control and security in their theory.

Information Security Theory by Horne, Ahmad and Maynard (2016)

Horne, Ahman and Maynard (2016), in their information security theory established the relationship between information and resources, controls and information, and threats and information. The following schematic illustrates this relationship:

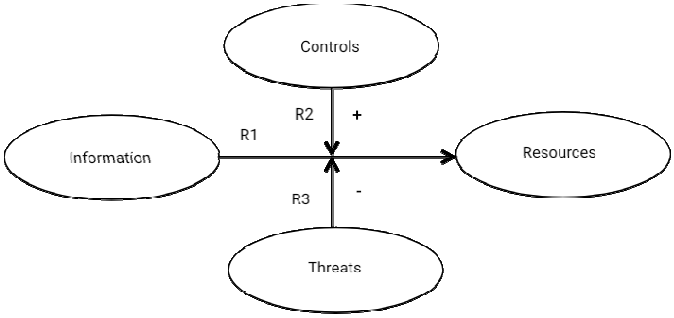

Figure 1: Schematic of Information Security
Source: Horne, Ahmad and Maynard (2016)

From Figure 1, arrows R1, R2 and R3 showcase the relationship between information and resources, controls and threats which could make or mar information becoming a resource. Horne, Ahman and Maynard explain that information is intangible in nature and has various levels of sensitivity. While non-sensitive information is not classified, sensitive information is classified in order of increasing importance such as: protected, confidential, secret and top secret. This classification considers levels of analysis such as: individual, group, organisational and inter-organisational. The levels of sensitivity and analysis help to determine which information is converted into a resource, and once information becomes a resource, its storage platform, access restrictions and sensitivity may upgrade, thus changing the level of analysis and protective controls. Once these levels of protection have been determined, suitable controls are to be implemented. Controls positively cause information to be protected and can be technical (computer based), formal (policies, procedures, rules) and informal (security, culture, education, training and awareness), and they help to prevent and detect attacks from threats. The implication is that without proper classification of information, security controls such as access control cannot be effectively implemented, and would lead to degradation of information, loss of value and damage to an organisation's resources and reputation.

Method

This study made use of a sequential exploratory mixed method survey research design. The sample population was 30 managers and information security officers of category 1 microfinance institutions in the North West Region of Cameroon. A binary questionnaire and an interview guide were the main instruments used to collect data. These were validated with the help of subject experts. Reliability was guaranteed using information security checklists such as those of ISO/IEC, and by use of the Kuder-Richardson's formula 20 (KR_{20}) to test internal consistency. A coefficient of 0.81 was obtained. Instruments were administered face-to-face and a 100% response rate registered. Data collected were analysed using descriptive statistics and thematic analysis. Pseudonyms were used to code participants and their institutions, with 'ISP1' to 'ISP15' used to represent the 15 Information Security Personnel (Officers), and 'M1' to 'M15' used to represent managers of the microfinance institutions under study. Research ethics was considered as participants were informed ahead of time, could partake voluntarily and findings placed at their disposal.

Findings and Discussions

Findings obtained from data gathered are presented and discussed in two main sections beginning with those on information classification and then access control.

Information Classification and Information Security Management in Microfinance Institutions

The first part of data obtained in relation to information classification is illustrated in Figure 2 below.

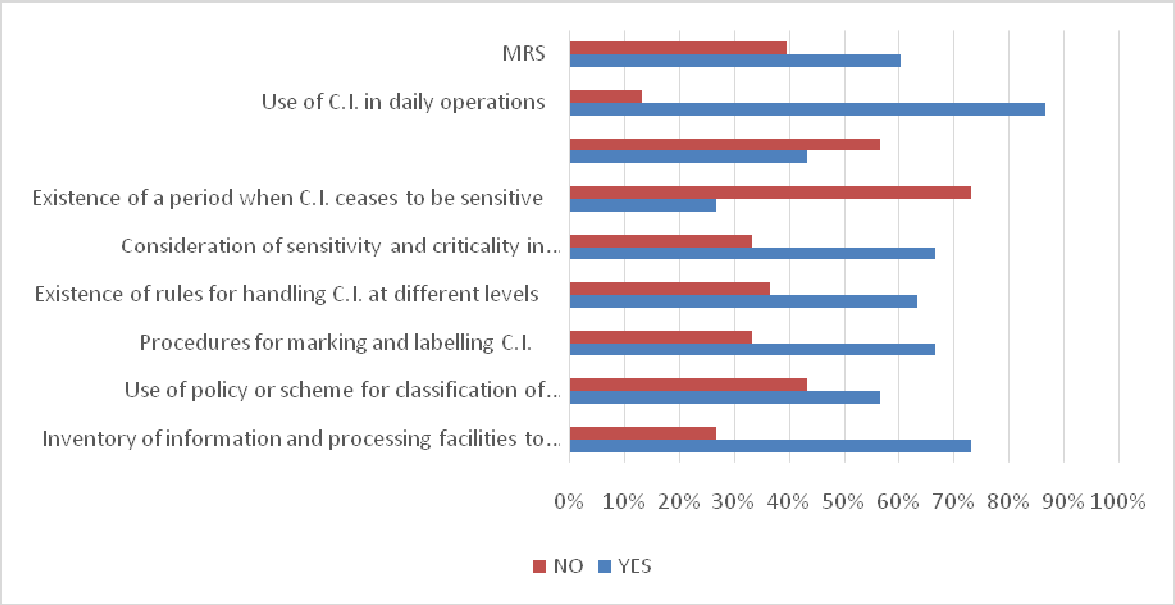

Figure 2: Information Classification in Microfinance Insti
Source: Data Analysis by the Researchers

Note: MRS = Multiple Response Set, C.I. = Classified Information

As presented in figure 2, most respondents (73.3%) agreed that their organisations do an inventory of information and processing facilities to identify and maintain important information assets. In addition, over half, (56.7%) agreed to the fact that their organisations have a policy or scheme governing classification of information assets. Again, 66.7% confirmed that there are procedures for marking and labelling classified information, and 63.3% accepted that their organisations have rules for handling classified information at different levels (processing, storage, transmission, declassification and destruction). Furthermore, 66.7% agreed that classification is done in terms of value, legal requirements, sensitivity and criticality of information to the organisation. On a lower note, only 29.7% agreed to the fact that there is a period when classified information ceases to be sensitive and 43.3% agreed that electronic and print information have the same procedures and guidelines for labelling and handling. Finally, 86.7% of respondents agreed to making use of classified information to facilitate daily operations in their organisations. As such, a Multiple Response Set of 60.4% (145) was realised for respondents who agreed and 39.6% (95) for those who disagreed to items in this section. This shows that almost 40% of the respondents were against existence of some information classification practices in their organisations. To get in-depth knowledge on importance of information classification, questions were posed requesting interviewees to list the types of information critical or sensitive to their organisations and how these are determined. The following themes were obtained as summarised on table 1 below:

Table 1: Themes Gathered on Information Classification

SN	Theme	Sub-Themes
1	Types of sensitive information	Members' account details, members' information, financial data, system transactions, board of directors decisions, collateral documents, staff information, important inquiries, total liquidity
2	Determining sensitivity	Account classes, common sense, financial positioning, exposure consequence, policies, scoreboard, apex body rule, ratio analysis

Types of Sensitive and Critical Information

The main sub-themes captured from participants on sensitive and critical information are; members' finances, members' information, financial data, system transactions, board of directors' decisions, collateral documents, staff information, enquiries and liquidity. Most participants clearly stated that members' finances are considered very sensitive and critical information. Participant ISP1 specified that; *"Financial information especially individual members' financial status' and account history are sensitive"*. Some interviewees also indicated that members' information and documents are considered critical and sensitive as supported by the following quote from ISP4; *"All members' or clients' information and documents are sensitive and critical to us"*. This implies that all information relating to clients have high value and require the highest level of protection.

Financial data is another sub-theme as obtained from quotes like; *"Organisational financial data and reports are sensitive"*, obtained from one of the managers. Systems transactions was also perceived to be sensitive and critical as supported by M5 who expressed that; *"System's transactions generated using the organisation's software on a daily basis"* are sensitive. Another manager, M10 was among those who identified board of directors' decisions as sensitive and critical as he expressed that;

"Important board of directors' decisions especially concerning staff, and loan files are sensitive information". Some of the participants believed that collateral documents are sensitive and critical to them as seen in the following statement put forth by M6; *"Collateral documents collected with loan files are important".*

Staff information was also considered sensitive and critical information as gotten from a few interviewees and substantiated by the statement; *"Employees' personal information and documents are important",* from M2. A few persons stated that inquiries are sensitive and critical to them. Participant M3 particularly considered sensitive information to be; *"Important inquiries from clients at the customer service".* Lastly, liquidity is another theme identified by ISP11 who +expressed that; *"The total level of liquidity in the office at a time is secret"*. The variety of themes generated implies that almost all information in these microfinance institutions is considered sensitive and requires some level of protection for the quality to be maintained. However, all of them cannot have the same level of sensitivity or criticality. Having a means to determine the level for each information asset is essential. As such, another interview question requested that interviewees give their opinions on what their organisations use to determine the sensitivity or criticality of information.

Determining Sensitivity and Criticality of Information

Of the eight sub-themes obtained on how sensitivity and criticality of information are determined, the main ones are; accounts, common sense and financial positioning. Participant ISP13, was one of those who indicated that they use account classes and numbers to determine criticality and sensitivity. ISP13 mentioned that; *"We use account classes which are broken down into classes 1 to 7, and account numbers".* Even though this theme was the most recurrent, it is insufficient since it does not consider information that is not related to accounts. In addition, some participants pointed out that they use common sense to determine sensitivity and criticality. ISP10 expressed that; *"No classification scheme is made available, but common sense and personal initiative is required and is better".* Common sense is also inadequate in classifying information because it does not follow standardised best practices in information classification and could leave out some elements. Again, some interviewees said that they use financial positioning such that, financial information is considered more sensitive than non-financial information. ISP8 in line with this said that; *"Financial positioning is the base on which we classify information".* It is a good method to determine the sensitivity of information in financial institutions but would be best if a scale is established to show the different types of information in each level.

Furthermore, a few interviewees stated that they consider the consequence of exposure as a determinant of sensitivity and criticality. This is supported by quotes like; *"The consequence of exposing the information is considered"* as expressed by M10. Another sub-theme on determining criticality and sensitivity is the use of policies. Support for this was captured in views like; *"We use policies put in place to be followed"* by ISP7. Using classification policies is a good practice but very few microfinance institutions made use of this. Again, scoreboard was stated by some as explained by M7; *"We use a scoreboard. We classify all information and score the risk involved on 5. Information with the highest risk are termed sensitive".* This method is good since it places information into various levels of sensitivity. Apex body rule as indicated by a few is another method and this is backed by responses like; *"We use the apex body rule of information classification"* from M5. From one of the managers, it was obtained that ratio analysis is used in determining criticality and sensitivity of information. In his words; *"We do a ratio analysis when classifying information"*. From the themes generated, it is evident that very few of the microfinance institutions under study had an established method in place which clearly distinguished the various levels of sensitivity or criticality of information. This implies that information classification processes are generally inadequate and with such, protection is not given to all information assets.

This study emphasises the role of information classification in information security management just as Horne, Ahmad and Maynard (2016) who explained that only sensitive information is classified in order of increasing importance, and that the level of sensitivity determines which information is a resource to an organisation and what protection it needs. Again, this study just like that of Kosutic (2014), lays emphasis on information classification in information security management. However, Kusotic duelled on four steps and established that levels of classification can be confidential, restricted, internal use and public use, while this study explored how classification is currently done by leaving it open for respondents to indicate which methods they use. With respect to this, it was disclosed that determining sensitivity is done in diverse ways by the microfinance institutions under study, which proves what Oscarson and Karlsson (2009) found that few developed guidelines for information classification exist. The diversity in ways of determining sensitivity among microfinance institutions under study could be attributed to the fact that each one chooses its own method, but because classified information can be dynamic and its value change with time as stipulated by Bergström and Åhlfeldt (2014), this study just like that of Al-Fedaghi (2008) is of the opinion that it is important to use accepted guidelines. Just like Ahmad, et. al. (2014), this study emphasises the need for levels of classification as bases for allocating access rights to information and processing facilities.

Access Control and Information Security in Microfinance Institutions

Summary of findings on access control in microfinance institutions is presented in the following chart:

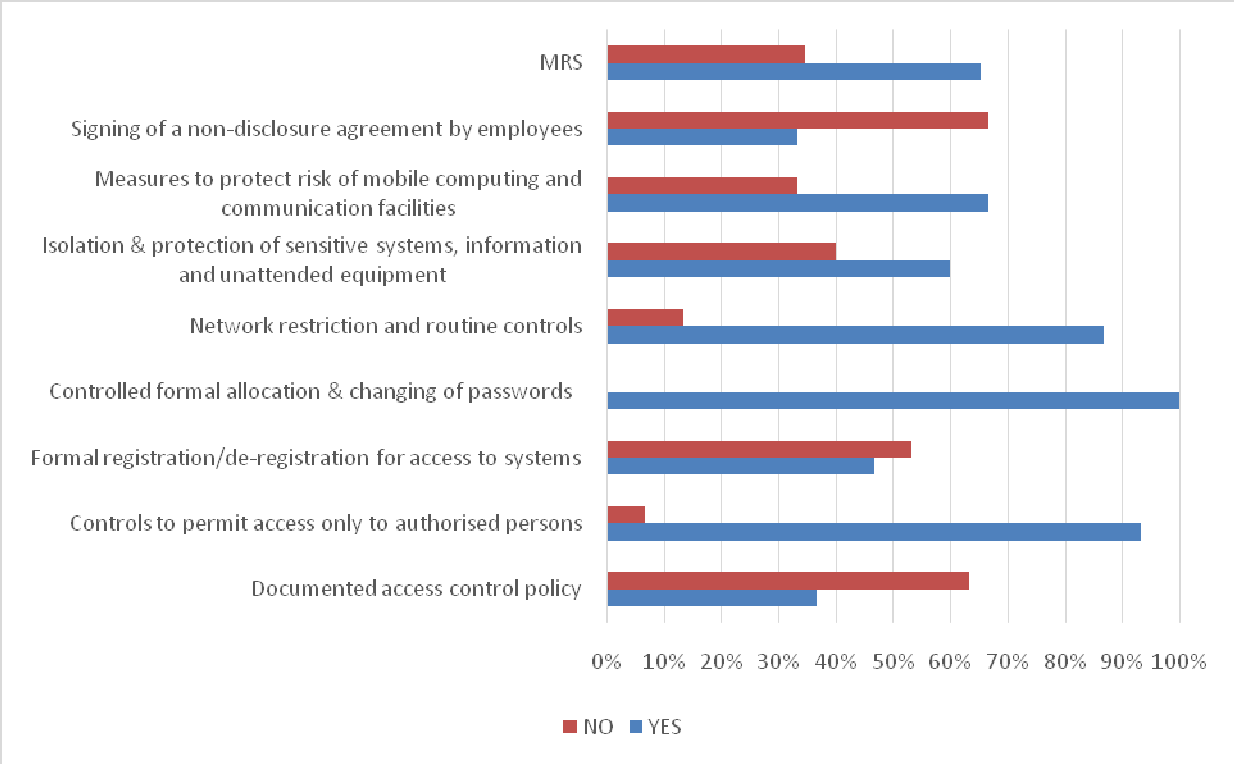

Figure 3: Access Control in Microfinance Institutions
Source: Data Analysis by the Researchers
Note: MRS = Multiple Response Set

From figure 3, barely 36.7% of the respondents agreed to having documented access control policies for information and information processing facilities. Interestingly, 93.3% agreed to have implemented controls to permit users have access only to information resources they have been authorised to use for their duties. On another level, less than half, 46.7% of respondents agreed that there is a formal user registration and de-registration procedure in place for granting and revoking access to information systems and services. On a remarkable note, all respondents (100%) agreed that allocation of passwords for each user is controlled through a formal process to guarantee password strength, periodic change and restricted access. There was a general believe by 86.7% that their network is restricted and routinely controlled according to the access control policy. Furthermore, 60% agreed that sensitive systems, information and unattended equipment are isolated in a dedicated environment and adequately protected, and 66.7% agreed that their organisations have security measures to protect risk of mobile computing and communication facilities. Last but not the least, only 33.3% agreed that employees sign a non-disclosure agreement for protecting the organisation's information assets. The Multiple Response Set for this section stood at 65.4% (157) for positive responses and 34.6% (83) for negative responses, implying that close to 40% of the respondents were for the fact that some elements of access control were missing in their organisations. In addition to this, some interview questions addressed access control, the first of which was on control of information and information processing facilities for home office employees.

Table 2: Themes Gathered on Access Control

SN	Theme	Sub-Themes
1	Access control for home office work	No control, instructions, passwords, privileged user access, coding
2	Technical and human-related issues of access control experienced	Technical: Electricity failure, network problems, machine breakdown, virus attacks Human-related: Unauthorized access, ignorance, loss, forgetfulness, outsider attacks, stubbornness

Access Control for Home Office Work

This aspect came about because employees of most financial institutions today are likely to take unfinished office work home thanks to Information and Communication Technologies (ICTs), which could jeopardise the security of confidential information. From interview responses as presented on Table 2, the five sub-themes obtained were; no control, instructions, passwords, user access and coding. Of these, most interviewees mentioned that there is "no control", since employees hardly carry work home. This was expressed in statements like; *"Staff are not permitted to carry work home so there is no control"* by M11. Again, some of the participants indicated that instructions from management are used to control employees who take work home, supported by excerpts like; *"Our organisation cannot control employees at home. However, they are reminded by management of the confidentiality requirements and penalties of negligence"* from the response of M5.

Other interviewees stated that passwords are used for control of work taken home. M10 explained that; *"For now, employees are not allowed to take work home except top*

management staff who have been provided with laptops that have passwords". Such passwords are meant to control access to information in their laptops. A few participants said that privileged user access rights are used to control work out of the office, substantiated by M3 in the statement; *"Through use and control of privileged user access rights".* Such rights are given only to a few trusted persons in the organisation. Lastly, M12 indicated that coding is used to control information when work is taken out of the office as supported by the statement; *"Carried home information are often coded for only employee access".*

From these themes, it is noticeable that technological measures to secure information when work is taken home are not sufficiently used. Very few mentioned use of passwords, privileged user accounts and coding to ensure the security of their information assets. Management instructions cannot sufficiently ensure adequate protection as some employees could be negligent and expose critical organisational information to outsiders, who may use it to damage the organisation in several ways. The next interview question on access control addressed technical and human-related issues experienced in line with access control, meant to extract some information security threats from participants.

Technical and Human-Related Issues of Access Control

Four sub-themes were generated on the technical side and six on the human side. With respect to technical issues, participants raised electricity failure as the main technical issue which affects access control. This was supported by M5, in the statement; *"Electricity failure disrupts the flow of information, making it to sometimes reach the central desk later than expected".* This could imply that electricity failure causes delays in accessing information and could cause some information in computers which had not been saved to be lost. Such disruptions in accessing information necessary for day-to-day functioning does not only affect the availability and integrity of information, but the organisation's effectiveness.

In addition, interviewees opined that network problems hinder access to information. Statements like; *"Network problems sometimes distort backing up and retrieval of members' information from the system",* from M7 support this theme. Delays caused by network failure could cause customers to be disgruntled and unsatisfied with services rendered. Furthermore, some interviewees said that the breakdown of machines obstructs access control. This was captured in statements like; *"Breakdown of machines prevents access to information"* from M3. Machine breakdown does not only prevent access to information but could expose critical information to danger especially if such machines are unattended to. Additionally, some participants said that virus attacks were an issue in access control as seen in quotes like; *"Inability to backup information due to virus attacks"* from ISP7. Such virus attacks have negative impact on ICT equipment in the work place and could hinder retrieval of information.

As for human-related issues, unauthorised access is one of the themes gotten from interviewees like ISP4, who explained that there is, *"Theft of important information without access permission."* Such unauthorised access could lead to changing and manipulation of information and could cost the organisation a lot monetarily. Interviewees again indicated ignorance as an issue of access control as participant M5 expressed that; *"Sometimes, employees unknowingly release sensitive information".* Other participants stated that loss of data/devices is one of the issues that had been encountered in relation to access control as clearly seen in the following response from ISP4; *"Devices get missing. Data is lost and exploited"*. The effects of this could be devastating to organisational information assets and the information security management programme.

Forgetfulness was also attributed as an issue of access control. An outstanding response from ISP7 supports this position *"A staff may forget and take backup devices home before closing time and employees sometimes forget passwords".* Forgetting to keep devices in their rightful and secure place could expose them to unauthorised parties. Some interviewees indicated that outsider attacks, mostly from relatives of clients was an issue of access control as supported by the statement; *"Some relatives of clients attack employees to demand balances in their relatives' accounts",* recorded from M11. Finally, stubbornness is another theme obtained as substantiated by the response from ISP6 in the statement; *"At times, employees may be stubborn and not want to implement a control measure for personal reasons".* These technical and human-related issues are an indication of the existence of information security threats common to many financial institutions around the world which if not properly handled could have devastating consequences on information security management and the organisation at large.

These findings are comparable with those of Horne, Ahmad and Maynard (2016) who presented threats that negatively cause information to degrade such as unauthorized access, changing of information and destruction of protective infrastructure, some of which have been experienced by some microfinance institutions under study. Contrary to ISO/IEC's point on non-negligence and password use, some of the microfinance institutions had experienced situations of negligence or forgetfulness of passwords and devices, a situation which is not good. Like Sinclaire (2013) suggested, experiences like forgetfulness or loss of storage devices in these institutions is the reflection of broken over-entitlement.

Conclusions and Recommendations

Conclusions

Since information classification and access control were shown to have inadequacies in the microfinance institutions under study, it could be inferred that information security management in these institutions is ineffective. Information classification and access control could therefore be considered positive predictors of effective information security management. Again, because of the non-existence of an appropriate and uniform scheme for information classification, existence of several technical and human-related issues of access control, it could be inferred that existence of a uniform classification scheme or schedule documented and communicated throughout the organisation, enough electricity supply, continues system maintenance and use of anti-virus software are possible predictors of effective information security management. If

these are not properly addressed, organisations' information security management goals could be unachievable.

Recommendations

Information security management programmes should target information classification and access control. Financial institutions should draft information classification schedules or schemes, and access control policies which suit their needs, with guidelines from standards like National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT) and ISO/IEC international standard for information security management. Information Security Officers or Information Managers should be introduced in microfinance institutions and their role should be taken seriously. Awareness programmes should be organised to help deter users from wrong practices, encourage good information management habits, and organisations should implement legal approaches like signing of non-disclosure agreements to deter users from malpractices.

REFERENCES

[1] Ahmad. A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective, *Computers & Security, 42*, 27 – 39.

[2] Al-Fedaghi, S. (2008). On information lifecycle management. In Asia-pacific services computing conference, 2008. *APSCC'08. IEEE* (pp. 335–342).

[3] Appleyard, J. (1998). *Information classification: a corporate implementation guide.* Auerbach Publications CRC Press LLC

[4] Ashenden, D. (2008). Information Security Management: A Human Challenge? *Information Security Technical Report, 13*(4), 195-201.

[5] Bergström, E., & Åhlfeldt, R.-M. (2014). Information classification issues. *In Secure it systems* (pp. 27–41). Springer.

[6] Gana, N. N., Abdulhamid, S. M., & Ojeniyi, J. A. (2019). Security Risk Analysis and Management in Banking Sector: A Case Study of a Selected Commercial Bank in Nigeria. *I.J. Information Engineering and Electronic Business*, 2, 35-43.

[7] Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). A Theory on Information Security, *Proceedings of the Australasian Conference on Information Systems, 2016*, Wollongong, Australia.

[8] Hu, V. C., Ferraiolo, D. F., & Kuhn, D. R. (2006). Assessment of Access Control Systems. *Interagency Report 7316, Computer Security Division*, National Institute of Standards and Technology.

[9] Hu, Q., Xu, Z. Dinev, T., & Ling, H. (2011). Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the ACM, Vol 54*, No. 6.

[10] ISO/IEC. (2005). ISO/IEC 27002-Information technology - Security techniques - Information security management systems - Requirements, *International Organisation for Standardization/International Electrotechnical Commission.* Geneva, Switzerland: ISO/IEC.

[11] ISO/IEC. (2009). ISO/IEC 27002:2009 - Information technology - Security techniques - Information security management systems - Overview and vocabulary. International Organisation for Standardization/International Electrotechnical Commission. Geneva, Switzerland: ISO/IEC.

[12] ISO/IEC. (2014). ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary, *International Organisation for Standardization/International Electrotechnical Commission.* Geneva, Switzerland: ISO/IEC.

[13] ISO/IEC. (2014b). ISO/IEC 27002 information technology – security techniques – code of practice for information security controls. ISO/IEC.

[14] Kosutic, D. (2014). Information Classification According to ISO 27001, Retrieved 31/08/2020 at 1:50pm from http://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso-27001/

[15] Nosworthy, J. (2000). Implementing Information Security in the 21st Century: Do you have the balancing factors? *Journal of Computer Security*, 19, 337-347.

[16] Oscarson, P., & Karlsson, F. (2009). A national model for information classification. In AIS SIGSEC workshop on information security & privacy (wisp2009), Phoenix, USA.

[17] Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, vol. 15*, pp. 112-133.

[18] Sinclair, S. (2013). Access Control in and for the Real World. *Technical Report TR2013-745 Department of Computer Science Dartmouth College*

[19] Tipton, H. F. & Krause, M. (Eds.). (2000a). *Information Security Management Handbook*. 4th ed., Vol. 1. Boca Raton, Florida: Auerbach Publications.

[20] Von Solms, R. (1998). Information Security Management (1): Why Information Security is so important. *Information Management & Computer Security, 6*(4), 174-177.

[21] Warkentin, M. & Willison, R. (2009). Behavioral and policy isues in information systems security: the insider threat. *European Journal of Information Systems (18),* 101 – 105. Doi:10.1057/ejis.2009.12.

[22] Zeneli, G. & Düsterhöft, F. (2016). Information Security in Banks and Financial Institutions, *Processional Evaluation and Certification Board, When Recognition Matters.* Retrieved 31/08/2020 at 1:54pm from http://pecb.com/pdf/article/87-information-security-in-banks-and-financial-institutions.pdf.