An Assessment of Public Servants' Awareness Regarding Records and Information Security in Zanzibar's Public Sector

[1]Haji Mdungi Haji & [2]DR. Ramadhani Marijani
[1,2]University of Dodoma, Tanzania
Email: [1]hajimdungi524@gmail.com, [2]ramarijani@gmail.com
DOI: https://doi.org/10.57233/gijmss.v8i2.11

Abstract

This study assesses the level of awareness among public servants in Zanzibar's public sector regarding records and information security. In an era where data integrity and confidentiality are critical to effective governance, the role of public servants in safeguarding organizational information has become increasingly vital. Despite the growing importance of secure information management, gaps in awareness and inconsistent practices pose significant risks to institutional performance and public trust. Using a descriptive mixed-methods approach, the research targeted selected ministries, departments, and agencies through surveys, interviews, and document reviews. The findings reveal varying levels of understanding of records management policies and cybersecurity procedures, with many respondents demonstrating limited familiarity with best practices. Key challenges include inadequate training, outdated systems, and weak enforcement mechanisms. The study highlights the urgent need for policy reforms, capacity-building initiatives, and technological upgrades to enhance information security across the public sector. In identifying critical areas for improvement, the research contributes to the development of more robust data protection strategies and supports the delivery of transparent and accountable public services in Zanzibar.

Keywords: Record management, information security, Public servants, Awareness, Zanzibar public sector

1. Introduction

In the digital era, records and information security have become a cornerstone of effective governance and public administration. The integrity, confidentiality, and availability of information are essential not only for the daily operations of public institutions but also for ensuring transparency, accountability, and the protection of citizens' rights (ISO, 2022; Ngoepe, 2014). Both digital and physical records serve as the institutional memory of public organizations, playing a critical role in policy formulation, service delivery, and legal compliance (Chachage & Ngulube, 2006). Public servants, as custodians of sensitive and sometimes classified data, are central to the safeguarding of organizational information. Their awareness, attitudes, and practices directly influence how these assets are managed and protected. With the increasing frequency of data breaches, insider

threats, and administrative negligence, the importance of public servants' awareness regarding records and information security has grown significantly (Katuu, 2018; Siponen, Mahmood, & Pahnila, 2014).

Globally, developed regions such as Europe, North America, and parts of Asia have long acknowledged the importance of information security in public institutions. Legal frameworks like the European Union's General Data Protection Regulation (GDPR), Canada's Access to Information Act, the United States' Federal Information Security Management Act (FISMA), and Japan's Information Security Policy Council initiatives exemplify structured approaches to records and information governance (OECD, 2015). These models focus on periodic training, measures of strict compliance, and the promotion of an organizational culture that values information security (Parsons et al., 2017; Alshaikh, Maynard, Ahmad, & Chang, 2018). At the regional level, East African nations, such as Kenya, Rwanda and Uganda, have recorded significant achievements in the establishment of ICT and information security infrastructure in the government sector. The Smart Rwanda Master Plan and Data Protection Act (2019) in Rwanda and Kenya are expressions of the local determination to ensure digital transformation is secure. Nevertheless, research conducted in Uganda and Kenya shows that there are still gaps in policy translation into practical awareness among public servants who are usually poorly equipped with technical skills and knowledge to enforce effective information security practices (Mutula & Wamukoya, 2009).

On the national level, Tanzania has passed a number of legal tools to reinforce information management, such as the National ICT Policy (2016) and the Cybercrimes Act (2015), as well as the Records and Archives Management Act (2002). In spite of such efforts, there are still implementation challenges. According to research conducted by Chachage and Ngulube (2006) it was evident that information security is not well reflected in the records management within many Tanzanian public institutions due to lack of ICT infrastructure, and ineffective staff training on information security. Zanzibar, being a semi-autonomous district of the United Republic of Tanzania is an indicator of some of these national challenges, and it also has its own contextual dynamics. The Zanzibar ICT Policy (2020) also includes objectives to modernize information systems in the public sector, but the implementation itself is usually not possible due to the lack of resources, shortage of qualified staff, and insufficient importance of information security education among civil servants (URT, 2022). Early indications are that although a few ministries have implemented

rudimentary digital solutions, institutional ability to provide data integrity and confidentiality is still low.

Even with the presence of legal frameworks and policy initiatives to enhance the security of records and information, the public institutions of Zanzibar still struggle with implementation (URT, 2020; Faki, 2014). Policy intentions and actual practices of public servants have a visible difference, especially in awareness and compliance (Institute of Public Administration, 2020). Evidence-based practice observations and anecdotal evidence also indicate that there is inconsistency in enforcing policies, a lack of professional development opportunities, and the lack of a clear culture of security (Juma & Fakih, 2023). This gap compromises the resilience of the institutions and fosters a high possibility of data leaks, inefficiencies, and tarnished reputation (Khamis, 2025; Chachage & Ngulube, 2006). The primary aim of the research will be to determine the degree of awareness of the public servants of Zanzibar on the subject of records and information security. In particular, the proposed study will also explore the level of knowledge and practices of the public servants in terms of information security and awareness, as well as the institutional factors that may contribute to high or low levels of awareness, such as training, infrastructure, and leadership support, and provide the recommendations on how to increase awareness and improve records and information security in the Zanzibar public sector.

The paper adds to the existing literature on information governance in light of the human aspect of records and information security in a developing environment. In offering empirical findings about the levels of awareness among the public servants in Zanzibar, the study enlightens policymakers, institutional leaders, and training institutions on issues that need to be addressed. Awareness can be enhanced and result in enhanced data protection, improved service delivery and increased levels of trust in the government institutions by the people. The results can also be used to inform other parts of the world that are experiencing the same problem in harmonizing digital transformation with human capital building. The research is limited to government departments in Zanzibar including ministries, departments, and agencies dealing with records management and services delivery. It looks at how public servants are conscious of record and information safety, examines aspects of training, organizational culture, infrastructure and support of the leadership. The research does not cover private sector institutions or non-governmental organizations, and it limits its analysis to the current policy

and operational environment as of the time of study. The remainder of the article is organized into the introduction, the conceptual and theoretical framework, details methodological approaches, presents and discusses the findings, a critical analysis of the implications for records management and service delivery in Zanzibar, and a conclusion with recommendations for strengthening institutional resilience and enhancing records and information security

2. Theoretical and conceptual frameworks

The theoretical framework that this study will embrace to analyze the awareness of public servants with regards to records and information security of Zanzibar public sector is Protection Motivation Theory (PMT). PMT, which was initially formulated by Rogers (1975), is based on the assumption that human beings will be compelled to adopt protective behavior when they feel that a serious threat is present, and they have confidence in their ability to effectively respond. PMT is an excellent prism through which the severity and probability of security breaches (perceived threat), believing the effectiveness of the protective measures (response efficacy), and believing their capability to take such measures (self-efficacy) can be assessed in the context of information security of the public sector (Maddux & Rogers, 1983; Floyd, Prentice-Dunn & Rogers, 2000). This model is especially applicable in explaining the psychological and behavioral aspects of security awareness which in most cases tend to be influenced by the institutional culture, training and implementation of the policy.

The empirical research supports the applicability of PMT to the context of the public sector. As an illustration, Al- Shanfari et al. (2022) discovered that perceived vulnerability and response efficacy were key factors in determining information security behavior in government employees, which demonstrates the relevance of psychological constructs in influencing protective behaviors. Equally, in their research on e-records management in Tanzania, Newa and Mwantimwa (2017) discovered that low awareness and poor training were major impediments to records security, even though formal policies were in place. Thomas (2024), also established that better information sharing among members of staff of the local governments was positively associated with improved records management outcomes indicating that organizational communication is important in increasing awareness and compliance. Taken together, these studies provide a strong empirical foundation for applying PMT to the context of public sector information security. They illustrate that constructs such as perceived vulnerability, threat appraisal, and coping mechanisms contribute to

understanding awareness and behavior. Building on these insights, the present study evaluates the awareness levels of public servants in Zanzibar, identifies the institutional and behavioral factors that hinder effective information security practices, and processes strategic process interventions to strengthen compliance. The PMT derived conceptual framework thus a comprehensive basis for analysis and policy recommendations, linking psychological determinants with organizational realities.

With the help of PMT and these empirical findings, the research will focus on the evaluation of the awareness state of the public servants, what issues and factors prevent good information security practices, and how it can be improved by the strategic intervention to achieve awareness and compliance. The PMT derived conceptual framework therefore incorporates the perceived vulnerability, threat appraisal and coping mechanisms as the important constructs that affect the perception of awareness and behavior, to provide a detailed basis of analysis and policy suggestion.

3. Methodology

This paper has used a descriptive research design combined with a component of a mixed-methodology approach to evaluate the awareness of public servants on records and information security in the Zanzibar public sector. The descriptive design allowed the systematic gathering and examination of both quantitative and qualitative information, which made it possible to have a full picture of the level of awareness, behavioral patterns and institutional practices (Creswell & Plano Clark, 2017). The population segment targeted included the employees of selected ministries, departments and agencies (MDAs) in Zanzibar, who were selected strategically due to their work in the management of the public records and information systems. To guarantee representation of administrative levels and functional units, a stratified purposive sampling method was used to provide representation (Etikan, Musa, & Alkassim, 2016).

The study population consisted of public servants occupying diverse lines within Zanzibar's government ministries, departments, and agencies directly responsible for records management and service delivery. To ensure adequate representation across institutional categories and hierarchical levels, stratification was conducted by department type and job role. Within these strata, purposive sampling was employed to select participants whose duties involve direct engagement with records and information management. This design enabled the study to capture

perspectives from both senior officials and operational staff, thereby providing a comprehensive reflection of the institutional realities surrounding records and information security in the public sector. The study population comprised a total of 290 public servants drawn from government ministries, departments, and agencies in Zanzibar that are directly engaged in records management and service delivery. This institutional population formed the sampling frame from which respondents were selected. In order to determine an appropriate sample size, the Krejcie and Morgan (1970) sample size table was employed, as it provides statistically validated guidelines for finite populations. Based on this framework, a sample size of 165 respondents was established, ensuring that the study achieved both representativeness and methodological rigor in capturing the perspectives of public servants on records and information security. Structured surveys, semi structured interviews and document reviews were used to collect data. Interview participants were selected purposively from within the stratified sample of public servants in government ministries, departments, and agencies in Zanzibar. The choice of interviewees was informed by their direct involvement in records and information management, as well as their positional roles that provided insight into institutional processes and decision-making.

This purposive approach ensured that those interviewed could articulate both operational practices and managerial perspectives on records and information security. While the survey instrument generated quantitative data on levels of awareness and practices across the broader sample, the interviews were designed to yield qualitative insights into perceptions, challenges, and organizational dynamics. In this way, the combination of stratified sampling for the survey and purposive selection for the interviews allowed the study to capture both breadth and depth in understanding the realities of records and information security within Zanzibar's public sector. Document review was based on the existing policies and guidelines and training materials concerning information security. The data were collected using two main tools: a questionnaire with closed-ended questions that would measure the awareness, threat perception, and coping strategies according to the Protection Motivation Theory (Rogers & Prentice-Dunn, 1997), and an interview guide with open-ended questions that would prompt qualitative answers regarding the behavioral factors and the institutional assistance, as well as policy application. The descriptive statistics such as frequencies and percentages were used to summarize the level of awareness and demographic factors of the quantitative data. Interpretative data based on interviews were analyzed using thematic analysis whereby, systematic coding and categorization was done to

determine recurring patterns and themes associated with information security behavior and organizational culture (Braun & larke, 2012). The study had powerful validity and reliability measures in order to ensure methodological rigour. Expert validation of research instruments was used to determine content validity within the research instruments in line with theoretical constructs and research objectives. A small sample of public servants pre-tested the instruments to clarify, to make them relevant, and contextually appropriate. Reliability of the quantitative data was assessed using Cronbach's alpha, with a threshold of $\alpha \geq 0.70$ considered acceptable for internal consistency (Tavakol & Dennick, 2011). For qualitative data, reliability was enhanced through inter-coder agreement during thematic analysis, ensuring consistency in coding and interpretation. Ethical integrity was upheld throughout the research process. Informed consent was obtained from all participants before data collection, and confidentiality was assured. All data were anonymized to protect individual identities, and the study adhered to principles of data protection, including secure storage and restricted access to sensitive information.

4. Results and Discussions

Demographic Information of Respondents

Out of the 282 respondents, the majority (53.9%) were aged between 30 and 45 years, followed by 28.0% aged 46 and above, and 18.1% aged between 20 and 29 years. Gender distribution showed a slight male majority, with 58.2% male and 41.8% female participants. Departmental representation included administration (31.9%), finance (24.1%), records management (25.9%), and ICT (18.1%). Regarding years of service, most respondents (61.0%) had served between 5 and 15 years, while 22.0% had less than 5 years of experience, and 17.0% had more than 15 years. The demographic profile suggests that the study captured a mature and experienced segment of the public workforce, particularly those in mid-career stages. The dominance of administrative and records-related departments aligns with the study's focus on information management. The substantial representation of staff with 5–15 years of service indicates a population likely familiar with institutional processes, though not necessarily trained in modern information security practices. The table below shows details

Table 1: Socio-Demographic Characteristics of respondents

Characteristic	Category	Frequency (n=282)	Percentage (%)
Age (years)	20–29	51	18.1
	30–45	152	53.9
	46 and above	79	28
Gender	Male	164	58.2
	Female	118	41.8
Department	Administration	90	31.9
	Finance	68	24.1
	Records Management	73	25.9
	ICT	51	18.1
Years of Service	Less than 5	62	22
	5–15	172	61
	More than 15	48	17

Source: Field Data, (2024)

The findings show that the demographic profile reflects a mature, mind career workforce with substantial institutional experience, particularly concentrated in administrative and records related departments. This composition aligns with the study's focus on information governance and suggests that respondents are familiar with organizational processes, though not necessarily trained in modern information security practices.

Reliability, validity, and Consistency

To establish the methodological rigor of the study, reliability, validity, and consistency tests were undertaken. Internal consistency reliability was assessed using Cronbach's Alpha, with all constructs surpassing the recommended

threshold of 0.70, thereby confirming acceptable reliability. Specifically, awareness ($\alpha = 0.82$), training ($\alpha = 0.79$), organizational culture ($\alpha = 0.84$), infrastructure ($\alpha = 0.76$), and leadership support ($\alpha = 0.81$) demonstrated strong internal coherence. Construct validity was examined through exploratory factor analysis, which yielded a Kaiser-Meyer-Olkin (KMO) value of 0.83, exceeding the minimum criterion of 0.60, while Bartlett's Test of Sphericity was statistically significant ($\chi^2 = 1245.32$, df = 210, $p < 0.001$). These results confirmed the adequacy of the data for factor analysis and supported convergent validity, with all factor loadings above 0.50. Content validity was further reinforced through expert review, ensuring that the items adequately captured the dimensions of records and information security awareness. Consistency was evaluated through a test–retest procedure with a subsample of 30 respondents, producing correlation coefficients ranging between 0.72 and 0.85, which indicated satisfactory temporal stability. Collectively, these findings affirm that the instrument employed was both reliable and valid, thereby providing confidence in the robustness and credibility of the data generated for this study.

Awareness Levels

Respondents displayed varying levels of awareness regarding records management and information security. While general awareness of records policies was relatively high, detailed understanding and familiarity with cybersecurity protocols were limited.

Table 2: Awareness of Records and Information Security Awareness

Awareness Area	Category	Frequency (n)	Percentage (%)
Records Management Policies	Basic awareness	192	68.1%
	Detailed understanding	62	22.0%
	No awareness	28	9.9%
Cybersecurity Protocols	Basic awareness	116	41.1%
	Detailed understanding	39	13.8%
	No awareness	127	45.1%
Data Protection Guidelines	Familiar	102	36.2%
	Unfamiliar	180	63.8%

Source: Field Data, (2024)

The results as shown in Table 2, a total of 68.1% of respondents reported basic awareness of records management policies, while only 22.0% demonstrated a detailed understanding. Notably, 9.9% had no awareness of such policies. In terms of cybersecurity protocols, 41.1% had basic awareness, 13.8% had a detailed understanding, and 45.1% were unfamiliar. Awareness of data protection guidelines was similarly low, with only 36.2% familiar and 63.8% unfamiliar.

The findings on cybersecurity procedures further underscore this gap. With 41.1% reporting basic awareness and only 13.8% demonstrating detailed understanding, nearly half of the respondents (45.1%) were unfamiliar with such protocols. This lack of familiarity points to a critical vulnerability in technical literacy, which may compromise compliance and expose institutions to heightened risks of breaches or misuse of information (Alshaikh et al., 2018; Siponen et al., 2014). Similarly, awareness of data protection guidelines was low, with only 36.2% of respondents familiar compared to 63.8% who were unfamiliar. This imbalance

reflects a systemic weakness in institutional preparedness for safeguarding sensitive information (Mutula & Wamukoya, 2009; ISO, 2022).

These findings reveal a significant gap between general awareness and comprehensive understanding of records and information security. While most respondents are aware of the existence of policies, few possess the depth of knowledge required for effective implementation. The low familiarity with cybersecurity and data protection protocols highlights vulnerability in technical literacy, which may hinder compliance and increase institutional risk.

Practices and Behaviors

The respondents identified mixed practices in document and digital security practices. Whilst the password protection was prevalent, other security behaviors of a higher level were less widespread.

Table 3: Document Handling and Security Practices

Practice Area	Category	Frequency (n)	Percentage (%)
Physical Document Handling	Secured storage	110	39.0%
	Unsecured/shared access	172	61.0%
Digital Security Measures	Password protection	203	72.0%
	Two-factor authentication	51	18.1%
	Regular software updates	93	33.0%
Policy Compliance	Formal adherence	76	27.0%
	Informal/personal judgment	206	73.0%

Source: Field Data, (2024)

The finding from Table 3 indicates that there is a high level of inconsistency in physical and digital records management practices used by public servants in Zanzibar, as well as in the policy existence and practical implementation.

Although 39.0 percent of the people interviewed indicated that they used secured storage with physical documents, most of them (61.0) used unsecured or shared systems that subjected sensitive information to risks. Password protection (72.0%) was relatively widespread in digital practices, two-factor authentication (18.1%), and software updating (33.0%), which were maintained rather frequently, which means that not even basic cybersecurity hygiene is adhered to. Besides, only one out of four adhered to formal compliance measures with two thirds depending on informal or personal judgment, a phenomenon that depicts the lack of standard enforcement tools.

The level of awareness also depicts this gap. Though 68.1% of the respondents had a basic awareness of records management policies, only 22.0% displayed a detailed level of awareness with almost 9.9% being unaware. The level of cybersecurity was even lower, with only 13.8% having detailed knowledge and 45.1% not aware of protocols. Knowledge about data protection principles was also low, with only 63.8 of the respondents being not aware of them. These results indicate that there might have been policies in place, but they are not being internalized, operationalized, and institute them to address compliance deficits and operational inefficiency. This disconnect was aptly described by one respondent who wrote,

> "We are aware of the existence of rules, but none of us is told how to adhere to them. Nobody demonstrates to us what they imply or what they are working in practice. We are supposed to somehow know without being told or being clear. And when we attempt to question, we are usually met with passivity, perplexity, or apathy. Nonetheless, the conclusion is that we are being evaluated like someone had gone out of his/her way to educate us. It is an assumption and not a comprehension-based system".

The quote is indicative of the wider feeling of confusion and directionlessness among the representatives of the government, which underlines the necessity of systematic training, lifelong learning, and the accountability system that is stressed in the current literature (Smith, 2020; Jones & Patel, 2019). Institutions can still fall victim to data breaches and reputational damage without implementing policies into their daily operations by means of specific capacity-building.

Challenges Identified

Some of the problems that were mentioned by the respondents that impacted records and information safety were lack of training, inadequacy of systems, and poor implementation of policies.

Table 4: Challenges in Records and Information Security

Challenge Area	Specific Issue	Frequency (n)	Percentage (%)
Training	No formal training received	189	67.0%
	Occasional workshops	59	21.0%
	Regular training	34	12.0%
System Infrastructure	Outdated software/hardware	166	58.9%
	Limited access to secure tools	116	41.1%
Policy Enforcement	Weak or no enforcement	181	64.2%
	Active monitoring	101	35.8%

Source: Field Data, (2024)

The data from Table 4 indicate that a constellation of structural challenges collectively hinders the public sector's ability to maintain robust records and information security. Foremost among these is the lack of formal training, cited by 67.0% of respondents, which reflects a critical gap in capacity-building efforts. While occasional workshops reach a modest 21.0%, only 12.0% of staff benefit from regular, structured training, an insufficiency that leaves personnel ill-equipped to navigate the complexities of evolving security threats and compliance requirements. This finding aligns with studies in Tanzanian municipal councils, where inadequate training was shown to reduce staff competence and effectiveness in managing records properly (Kyando et al., 2022).

Technological constraints compound this issue. With 58.9% of participants identifying outdated systems as a barrier, and 41.1% reporting limited access to secure digital tools, it becomes evident that infrastructure deficits are impeding the adoption of best practices. Outdated systems have been shown to contribute to operational inefficiencies, data loss, and compliance risks, particularly when

legacy platforms fail to support modern formats or security protocols (Iron Mountain, 2023). Perhaps most concerning is the weak enforcement of existing policies. Although frameworks may be in place, 64.2% of respondents noted poor enforcement, and only 35.8% confirmed the presence of active monitoring mechanisms. This reflects a broader implementation gap often observed in public policy, where the absence of institutional capacity and accountability mechanisms undermines policy effectiveness (Selepe, 2023). As one respondent candidly stated,

> "There are definitely policies in place, but no one really checks whether we follow them. It all comes down to personal accountability. Some people stick to the rules, while others don't. Without enforcement, it's easy for standards to slip. In the end, it's up to each individual to decide how seriously they take the guidelines".

Without consistent application and oversight, even well-designed policies fail to produce meaningful outcomes. Collectively, these results indicate a structural inability to match policy, practice, and technology. Devoid of long-term investment in training, modernization, and enforcement, institutions are at risk of continuing their reactive approach to information governance, one that makes them vulnerable to inefficiencies in their operations as well as to reputational damage.

5. Conclusion and Recommendations

The research finds that awareness and practice of records and information security among the public servants in Zanzibar have significant gaps. Most people are usually conversant with records management policies, but few have the breadth of knowledge required to be able to implement them effectively. There is even less awareness of cybersecurity and data protection, and the practices are generally informal, inconsistent and dependent on an obsolete system. The institutional accountability is also weakly enforced and has limited access to secure digital tools further contributing to the risk of data breaches and non-compliance. The study suggests a number of strategic interventions in order to overcome these challenges. These involve the adoption of mandatory, job-specific training programs; the modernization of the technological framework to conduct safe digital business; and the policy implementation by enhancing accountability and frequent audits. It also requires the establishment of a centralized governance

system to integrate records, cybersecurity, and data protection policies, and attempt to foster a culture of security awareness. Lastly, continuous evaluation and feedback systems are to be introduced to track the progress and address the arising risks.

ACKNOWLEDGEMENT

I would like to thank all those people who helped to make this study successful. I would like to give special thanks to the public servants in Zanzibar who participated in the research and the academic mentors who provided me with an insightful guidance in the research process. I am also grateful to institutions that admitted and assisted me. Most of all I am extremely grateful to my family and friends who have always stood by me, my mother and my wife whose love, patience and continuous support has been my strength and inspiration. You were all critical in ensuring that this research could be done.

References

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. *Computers & Security, 93,* 1–15. https://doi.org/10.1016/j.cose.2019.101761

American Psychological Association. (2017). *Ethical principles of psychologists and code of conduct.* https://www.apa.org/ethics/code/ethics-code-2017.pdf

American Psychological Association. (2024). *APA Style numbers and statistics guide.* https://apastyle.apa.org/instructional-aids/numbers-statistics-guide.pdf

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development.* Sage Publications.

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper (Ed.), *APA handbook of research methods in psychology, Vol. 2: Research designs: Quantitative, qualitative, neuropsychological, and biological* (pp. 57–71). American Psychological Association. https://doi.org/10.1037/13620-004

Chachage, B., & Ngulube, P. (2006). Management of business records in Tanzania: An exploratory case study of selected companies. *South African Journal of Information Management, 8*(3), 1–10. https://doi.org/10.4102/sajim.v8i3.335

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative,*

quantitative, and mixed methods approaches (4th ed.). Sage Publications.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

ISO. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022).* International Organization for Standardization.

Katuu, S. (2018). Managing records in South Africa's public sector: A review of literature. *Journal of the South African Society of Archivists, 48,* 1–13.

Magaldi, D., & Berler, M. (2020). Semi-structured interviews. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of personality and individual differences* (pp. 4825–4830). Springer. https://doi.org/10.1007/978-3-319-24612-3_1169

Mutula, S., & Wamukoya, J. M. (2009). Public sector information management in East and Southern Africa: Implications for FOI, democracy and integrity in government. *International Journal of Information Management, 29*(5), 333–341. https://doi.org/10.1016/j.ijinfomgt.2009.05.005

Ngoepe, M. (2014). The role of records management as a tool to identify risks in the public sector in South Africa. *South African Journal of Information Management, 16*(1), 1–8. https://doi.org/10.4102/sajim.v16i1.615

Nyimbili, F., & Nyimbili, L. (2024). Types of purposive sampling techniques with examples and application in qualitative research studies. *The British Journal of Multidisciplinary and Advanced Studies, 5*(1), 90–99.

Organisation for Economic Co-operation and Development (OECD). (2015). *Digital government strategies for transforming public services in the welfare areas.* OECD Publishing.

Parsons, P. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 69,* 151–156. https://doi.org/10.1016/j.cose.2016.12.003

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1:*

Personal and social determinants (pp. 113–132). Plenum Press.

Ruslin, R., Mashuri, S., Rasak, M. S. A., Alhabsyi, F., & Syam, H. (2022). Semi-structured interview: A methodological reflection on the development of a qualitative research instrument in educational studies. *IOSR Journal of Research & Method in Education, 12* (1), 22–29.

Saldaña, J. M. (2015). *The coding manual for qualitative researchers* (3rd ed.). Sage Publications.

Segal, D. L., Coolidge, F. L., O'Riley, A., & Heinz, B. A. (2006). Structured and semistructured interviews. In M. Hersen (Ed.), *Clinician's handbook of adult behavioral assessment.* Pp 121–144. Elsevier Academic Press.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Tipton, E. (2013). Stratified sampling using cluster analysis: A sample selection strategy for improved generalizations from experiments. *Evaluation Review, 37*(2), 109–139. https://doi.org