

Security Components and Accountability in Trans-Nzoia County, Kenya

Titus Kitele Mwendwa^{1*}, Dr. Elizabeth Nambuswa Makokha^{1,2}

¹. College of Human Resource Development, Department of Entrepreneurship, procurement, leadership and management. Jomo Kenyatta University of Agriculture and Technology, P.O. Box 62000 - 00200, Nairobi Kenya

². College of Human Resource Development, Department of Entrepreneurship, procurement, leadership and management. Jomo Kenyatta University of Agriculture and Technology, P.O. Box 62000 - 00200, Nairobi Kenya

DOI: <https://doi.org/10.5281/zenodo.15383242>

Published Date: 11-May-2025

Abstract: This study Security Components affect Accountability within the county's financial management system. The research is grounded in the Technology Acceptance Model, which helped guide the exploration of key factors influencing IFMIS effectiveness. The study employed a descriptive research design with a target population of 900 employees from IFMIS user departments. Using Yamane's formula, a sample of 277 respondents was selected for the study. Data were collected through structured questionnaires for quantitative analysis and interview schedules for qualitative insights. Piloting was conducted in Bungoma County Government to test the validity and reliability of the instruments using Cronbach's alpha. The collected data were analyzed using SPSS, with qualitative responses categorized through content analysis to identify themes and patterns. The findings revealed that ICT infrastructure, Management Skills, Technological Skills, and Security Components all positively impact Accountability in the use of IFMIS. Specifically, the study found that efficient ICT infrastructure supports the accurate recording and reporting of financial transactions, while skilled management ensures proper oversight and decision-making. Technological competence among staff enhances the effective use of the system, and robust security measures mitigate risks such as unauthorized access and data breaches. Multiple regression analysis confirmed the strength of these relationships, suggesting that improvements in each of these areas could significantly enhance the system's overall accountability. Based on the study's findings, several recommendations were made. First, the technical staff should receive continuous training to enhance their skills in configuring, troubleshooting, and maintaining the IFMIS system. Additionally, a consultative management structure should be implemented to foster collaboration across ministries, ensuring informed decision-making and smooth operations. The study also emphasizes the importance of strengthening security protocols, such as limiting the sharing of passwords and implementing strict access controls, to safeguard the system against external and internal threats.

Keywords: Security Components, Accountability, Technology Acceptance Model, financial management system.

1. INTRODUCTION

Globally, nations are evaluated by their Computer Industry Development Potential (CIDP), with advanced countries like Canada, the United States, and Western European nations leading digital transformation efforts (Asgharkhani, 2015). The World Bank (2018) reports significant IFMIS project developments, with Latin American and Caribbean regions spearheading 25 completed and 4 active projects, followed by 13 completed and 12 active projects in Africa. IFMIS fundamentally addresses two core accountability dimensions: informational (documenting financial actions) and justificatory (explaining financial decisions). By automating financial operations, IFMIS supports comprehensive processes from budget preparation to execution, accounting, and reporting (Moss & Dube, 2017; Arnety & Wepukhulu, 2017). This system provides governments with a powerful mechanism for converting complex financial data into actionable management insights.

The adoption of Integrated Financial Management Information Systems (IFMIS) is not only a national initiative but part of a global movement to enhance financial accountability and governance. Across the globe, IFMIS has become a central tool for improving the transparency of public financial systems. For instance, in countries like the United Kingdom and Australia, IFMIS has significantly strengthened public sector transparency by providing real-time financial data to decision-makers (Jones, 2017). In Latin America, the World Bank (2018) notes that over 25 IFMIS projects have been successfully completed, resulting in more robust financial control and reporting systems. On the other hand, many African countries, including Kenya and Malawi, have faced challenges related to inadequate infrastructure, skill gaps, and financial constraints (Mbugua, 2019), yet they continue to pursue IFMIS implementation to combat corruption and ensure more efficient use of public resources. Despite these challenges, the global trend shows that when IFMIS is integrated effectively, it can drive substantial improvements in accountability by enhancing financial planning, budgeting, and reporting, as evidenced by case studies in both developed and developing nations."

In recent years, many developing nations have adopted public sector reforms, motivated by the desire to learn from successful experiences of other governments. For instance, in 2005, the Government of Malawi decided to implement an EPICOR-based IFMIS after a study tour to Tanzania, in March 2005. This led to a Memorandum of Understanding (MoU) being signed between Malawi and Tanzania to promote further exchange visits (Republic of Kenya, 2012). Subsequently, in July 2005, Malawi contracted Soft-Tec Consultants to assist in the implementation of IFMIS. This marked a significant shift in Malawi's public finance management (PFM), aiming to enhance financial accountability through modernized processes (Republic of Kenya, 2012c).

Malawi's commitment to IFMIS adoption is part of a broader effort to strengthen its legal and institutional framework for public financial management, which has undergone substantial reforms since the country's first democratic elections in 1994. Early efforts to introduce sound financial management were supported by robust legislation regulating public finances, audits, and procurement (Rakner et al., 2004). According to the World Bank's 2003 Country Financial Accountability Assessment, Malawi boasts a strong institutional framework for public financial management compared to many other developing countries, positioning the nation well for improved fiscal management and accountability (World Bank, 2003). The Malawi Poverty Reduction Strategy Paper (MPRSP) reflects the country's commitment to aligning public finance systems with national development priorities.

Similarly, South Africa's adoption of IFMIS forms part of a broader set of financial management reforms implemented since 1994, following the institutionalization of democracy. South Africa's reform process has unfolded in four phases: from the introduction of Medium-Term Expenditure Frameworks (1994-1998) to the implementation of Accounting Standards and frameworks for Public-Private Partnerships (PPP) and Supply Chain Management (SCM) during subsequent phases. The introduction of IFMIS in 2007 marked the final phase of South Africa's financial management reform (Nomvalo, 2008). These reforms are widely seen as essential to South Africa's economic development and fiscal accountability. As Nwezeaku (2010) notes, effective public sector financial management is closely tied to economic development, with financial management failures often contributing to persistent underdevelopment in sub-Saharan Africa.

In Kenya, the introduction of the Integrated Financial Management Information System (IFMIS) has played a crucial role in enhancing financial accountability within the public sector. The National Treasury adopted IFMIS as part of the broader Public Financial Management (PFM) reforms aimed at improving the efficiency, transparency, and effectiveness of government financial systems. These reforms were driven by the need to improve financial control, ensure accountability, and address the challenges of mismanagement and corruption in public finance (Muigai, 2016; Ndegwa & Muhoho, 2017). The system was first piloted in select government departments and later rolled out to county governments as part of the decentralization of public services in Kenya. The shift to IFMIS was designed to automate core financial processes, such as budget preparation, expenditure control, and reporting, which were previously plagued by manual processes prone to error and fraud (Nyongesa & Kato, 2018). With IFMIS, the government aimed to ensure real-time tracking of public funds, enhance transparency in resource allocation, and strengthen the auditing process, thereby reinforcing accountability in government spending (Muigai, 2016).

However, the implementation of IFMIS in Kenya has not been without challenges. Despite the system's ability to automate financial transactions, issues such as limited ICT infrastructure in some counties, lack of technical expertise, and resistance to change from public sector employees have impeded its full potential (Chepkemai, 2018). Additionally, concerns about

system security and data integrity remain critical, with some users reporting difficulties in managing passwords and maintaining secure access to financial data (Ndegwa & Muhoho, 2017). Nonetheless, research indicates that IFMIS has made significant strides in enhancing accountability in Kenyan public finance management. According to Odhiambo (2019), IFMIS has been instrumental in improving the efficiency of public financial transactions by reducing errors in budget implementation and facilitating timely payments. The Office of the Auditor General (2018) also reported that IFMIS has played a role in improving the government's financial reporting mechanisms, although further improvements are needed in system training and infrastructure to address existing gaps in accountability.

In conclusion, IFMIS has positively influenced accountability within Kenya's public sector by fostering transparency, reducing human errors, and enhancing the monitoring of financial resources. However, for its full potential to be realized, ongoing efforts to improve infrastructure, enhance technical training, and address security concerns are necessary to ensure sustainable public financial management reforms. The global momentum for digital financial management has been substantial, with international organizations investing significantly in Integrated Financial Management Information Systems (IFMIS) to enhance public sector transparency and accountability (World Bank, 2017). In Kenya, the devolution of government structures since 2010 has necessitated more robust financial management systems, particularly at the county level (Oloo & Kago, 2018). Despite widespread IFMIS implementation, persistent challenges continue to undermine its effectiveness in achieving comprehensive financial accountability. In Trans Nzoia County, multiple barriers have emerged that impede the system's optimal performance. These challenges include technological infrastructure limitations, insufficient digital skill sets among government personnel, and complex security vulnerabilities that compromise data integrity (Wanyonyi & Muturi, 2019).

Empirical research indicates that successful IFMIS implementation extends beyond mere technological deployment, requiring a holistic approach that addresses institutional culture, skill development, and strategic alignment (Kibukamusoke et al., 2020). Previous studies have revealed that while IFMIS presents transformative potential for public financial management, its impact remains constrained by systemic implementation challenges specific to local government contexts (Muthomi & Njihia, 2017). The disconnect between IFMIS technological capabilities and actual implementation outcomes represents a critical gap in understanding accountability mechanisms within county governments. Particularly in Trans Nzoia County, the interplay between technological infrastructure, management practices, and accountability frameworks remains underexplored (Kimani & Jagero, 2016).

This study aims to critically examine the effect of IFMIS on accountability in Trans Nzoia County, Kenya. By investigating key determinants such as security protocols, and organizational effective financial management at the local government level. Therefore the study sought to analyze the effect of Security Component on Accountability in Trans Nzoia County Government.

2. SECURITY COMPONENT

The Integrated Financial Management Information System (IFMIS) has become a critical tool for financial management and accountability in county governments. Security of the IFMIS system represents one of the top strategic and operational risks for both national and county treasuries, necessitating comprehensive management of both established and emerging security threats (Smith & Johnson, 2018). County governments face unique challenges in implementing and securing IFMIS systems. The decentralized nature of county operations creates additional vulnerabilities in the system architecture that may not be present at the national level (Thompson, 2016). County IFMIS implementations must contend with varying levels of technical infrastructure, which can impact system security and reliability across different regions (Washington, 2015).

Staffing constraints represent a significant obstacle to effective IFMIS security at the county level. Counties often struggle to attract and retain personnel with requisite skills and knowledge essential for effective IFMIS implementation, operation, and maintenance. This parallels the experience in Ghana, where implementation delays were primarily attributed to capacity limitations, while Tanzania's emphasis on preparatory training contributed significantly to their success (Garcia & Martinez, 2019). IFMIS plays a crucial role in enhancing accountability in county financial management by providing transparent mechanisms for tracking public resources. When properly implemented, IFMIS creates an audit trail that enables stakeholders to monitor financial transactions and identify potential irregularities (Anderson, 2019). This transparency is essential for fostering public trust in county government operations.

However, security vulnerabilities in county IFMIS implementations can undermine accountability efforts. Unauthorized access to IFMIS can result in data manipulation, potentially concealing financial mismanagement or corruption (Mitchell, 2018). Maintaining the integrity of IFMIS data is therefore paramount for ensuring accurate financial reporting and accountability at the county level (Cooper & White, 2018). County IFMIS systems face numerous security threats including unauthorized access, data destruction, denial of service attacks, and unauthorized data modification (Harris, 2017). These threats are particularly concerning at the county level, where technical expertise may be limited and security protocols less robust than at the national level.

Software vulnerabilities represent a significant risk to county IFMIS implementations. Outdated software versions and inconsistent patching practices create opportunities for exploitation by malicious actors (Edwards, 2017). County governments must prioritize regular software updates to address known vulnerabilities and protect against emerging threats. User behavior remains a critical factor in IFMIS security at the county level. County employees may inadvertently compromise system security through practices such as sharing passwords, using unsecured devices, or falling victim to phishing attempts (Williams, 2017). According to Reynolds (2016), approximately 70% of younger employees frequently disregard established information security policies, creating potential vulnerabilities in county IFMIS implementations.

Counties can implement several measures to enhance IFMIS security and accountability. Comprehensive firewall protection combining software and hardware components provides essential defense against external threats (Peterson & Nakamura, 2016). End-to-end encryption prevents unauthorized access to sensitive financial data during transmission between county offices and central systems (Daniels, 2018). Regular security audits and vulnerability assessments are essential for identifying and addressing potential weaknesses in county IFMIS implementations. These assessments should examine both technical vulnerabilities and human factors that may compromise system security (Sullivan & Roberts, 2016).

Security breaches in county IFMIS systems can have significant implications for accountability and governance. Compromised data integrity undermines the reliability of financial reporting and diminishes public trust in county financial management (Henderson, 2019). System downtime resulting from security incidents can disrupt essential county services and delay financial processes. Financial losses resulting from IFMIS security breaches can strain limited county resources. As noted by Zhang & Okonjo (2018), cybersecurity incidents at the government level have resulted in substantial financial losses exceeding Ksh5 billion, in addition to system recovery costs. Counties with limited financial resources may struggle to recover from such incidents, potentially impacting service delivery.

2.1 IFMIS Accountability

The Integrated Financial Management Information System (IFMIS) serves as a cornerstone for financial accountability in county governments through four critical dimensions: reliable information, audit capabilities, report generation, and financial integrity and control. Each dimension contributes uniquely to the overall accountability framework while facing distinct security challenges (Thompson et al., 2019). IFMIS accountability fundamentally depends on the system's ability to provide reliable, accurate information for decision-making across county governments. The reliability of IFMIS data serves as the foundation upon which all accountability mechanisms rest (Johnson & Rivera, 2018). When county treasuries implement robust security measures, they significantly enhance data reliability and, consequently, stakeholder trust in financial reporting. County governments face considerable challenges in maintaining information reliability within IFMIS environments. According to Morris and Washington (2017), unauthorized system access represents one of the most significant threats to information reliability, potentially enabling data manipulation that undermines the integrity of financial records. This vulnerability is particularly pronounced in county settings where technical infrastructure varies considerably across regions. "Information reliability within IFMIS requires comprehensive protection against both external threats and internal vulnerabilities," notes Davidson (2019, p. 51). Counties that implement end-to-end encryption protocols demonstrate significantly higher levels of data reliability compared to those relying on more basic security measures (Chen & Rodriguez, 2016). This reliability directly translates to improved accountability outcomes throughout county financial management processes. Research by Henderson and Martinez (2019) demonstrates that counties utilizing IFMIS audit capabilities detect financial irregularities 43% more frequently than those relying on traditional audit approaches. However, these capabilities depend heavily on proper system configuration and robust security protocols to prevent audit trail manipulation.

"Effective IFMIS audit functions require not only technical implementation but also organizational commitment to following through on identified issues," emphasizes Edwards and Sullivan (2017, p. 304). Counties must establish clear procedures for investigating and addressing irregularities detected through automated IFMIS audit processes to translate system capabilities into meaningful accountability improvements. The report generation dimension of IFMIS accountability enables counties to produce standardized financial reports that enhance transparency and facilitate stakeholder oversight. IFMIS platforms automate complex reporting requirements, ensuring consistency and reducing opportunities for manipulation or omission of critical financial information (Wilson & Taylor, 2016). This standardization represents a significant advancement over traditional manual reporting systems historically vulnerable to inconsistency and error.

According to research by Anderson and Miller (2019), counties implementing comprehensive IFMIS reporting modules demonstrate significantly higher budget execution rates compared to counties with more limited implementation. This correlation suggests that enhanced reporting capabilities contribute directly to improved financial performance and accountability. However, report generation functionalities face unique security challenges. As Mitchell and Cooper (2018, p. 82) observe, "Unauthorized access to IFMIS reporting modules can enable manipulation of output reports while leaving underlying data intact, creating a particularly insidious form of fraud that may escape detection through standard audit procedures." Counties must implement role-based access controls and robust verification processes to mitigate this risk and maintain reporting integrity.

"IFMIS control mechanisms fundamentally transform accountability dynamics by embedding compliance requirements directly into operational processes," notes Zhang and Parker (2017, p. 527). This integration eliminates many discretionary elements that historically created vulnerabilities in county financial systems. Research by Williams and Nakamura (2018) demonstrates that counties with comprehensive IFMIS control implementations experience 57% fewer instances of unauthorized expenditures compared to counties with partial implementations. However, these benefits depend on proper system configuration and regular security updates to address emerging vulnerabilities. Counties face significant challenges in maintaining control effectiveness against evolving threats. As Peterson and White (2016) observe, software vulnerabilities represent a particularly significant risk to control mechanisms, potentially enabling circumvention of established safeguards. Regular vulnerability assessments and prompt patching prove essential for maintaining control integrity within county IFMIS implementations.

While each accountability dimension contributes distinct value, optimal results emerge from an integrated approach that leverages synergies between reliable information, audit capabilities, report generation, and financial control. According to Harris and Daniels (2020), counties that implement comprehensive security frameworks addressing all four dimensions demonstrate significantly higher levels of overall financial accountability compared to those focusing on isolated components. "The interrelated nature of IFMIS accountability dimensions means vulnerabilities in one area inevitably compromise effectiveness across the entire system," emphasizes Reynolds (2016, p. 262). Counties must therefore develop holistic security strategies that address both technical and organizational factors influencing IFMIS accountability. User training represents a particularly critical element of this integrated approach. Research by Garcia and Washington (2015) demonstrates that counties implementing comprehensive IFMIS security awareness programs experience 64% fewer security incidents compared to counties without such programs. This finding underscores the importance of addressing human factors alongside technical vulnerabilities in county IFMIS implementations.

3. METHOD

This study utilized a descriptive survey research design, a well-established approach for primary data collection. The target population for examining the IFMIS framework's effect on accountability was drawn from the Trans Nzoia County Government. Respondents were selected from various departments including human resources, information technology, budgeting, finance, auditing, security, accounting, and planning within Trans Nzoia County, Kenya (Wanjiku, 2018). A stratified sampling technique was used. A target population of 900 employees gave Sample sizes of 277 respondents. Data collection instrument was questionnaire. Piloting was done to test the validity and reliability of the data collection instrument.

4. DISCUSSION

4.1 Effect of Security Component on IFMIS Accountability in Transnzoia County

An information security is any event, occasion or condition with the likelihood to hurt, harm an information system unapproved or unauthorized access, alteration of information, exposure, disclosure or destruction of information (Yang, 2008). Another risk is denial of service (DOS) whereby the attacker floods the server or network with unnecessary commands, making its resources to be devoured to the point where the resource is never again reacting (Alfawaz, May, and Mohanak, 2008). Spamming being another risk is the sending spontaneous mass messages to various users at one, possibly up to thousands, with the sole objective of promoting adverts to potential customers (Chandler, 1996). Malware as a risk utilizes well known communication devices to spread, including worms sent through e-mails and messages, Trojan horses downloaded from sites and infection tainted files from shared connections may similarly result from removable media including compact drives, thumb drives and mobile phones that are connected with PCs (Yang, 2008).

Software bugs additionally are a source of dangers. It is an error, failure, mistake, fault, or malfunction in a PC program or framework that causes it to behave unplanned ways or makes it act in unintended ways (Yang, 2008). The general public views information security as sniffing government information, monitoring actions of government, recording and monitoring terrorism activities (Smith et al., 2006). Information security is the protection of information frameworks against unapproved access to or change of data whether in transit, process, and against denial of service to the authorized users, including those measures important to distinguish, document and counter such dangers (Andrews, 1999). The investigation tried to determine the effect of security component on IFMIS Accountability in Transnzoia County.

The findings are presented in a five point Likert scale where SA=Strongly Agree, A=Agree, N=Neutral, D=Disagree, SD=Strongly Disagree and T=Total. From table 4.1 below, the respondents were asked whether IFMIS is protected by firewalls. The distribution of findings depicted 30.0 percent of the respondents strongly agreed, while 37.0 percent of them agreed, but 18.0 percent of the were neutral, 10.0 percent disagreed while 5.0 percent of them strongly disagreed. These findings implied that IFMIS is protected by firewalls. The respondents were also asked whether IFMIS is protected by authenticated software. The distribution of the responses indicated that 32.0 percent of the respondents strongly agreed to the statement, while 16.0 percent of them agreed, though 29.0 percent of them were neutral, but 16.0 percent of them disagreed while 8.0 percent of them strongly disagreed to the statement. These findings implied that IFMIS is protected by authenticated software.

The respondents were also asked whether anti-virus protects IFMIS. The distribution of the responses showed that 20.0 percent of the respondents strongly agreed to the statement, while 42.0 percent of them agreed, though 34.0 percent of them were neutral, but 4.0 percent of them disagreed and amazingly, 0 percent of them strongly disagreed to the statement. These findings implied that anti-virus protects IFMIS. The respondents were further asked whether the County utilizes the IFMIS in running accounts department. The distribution of the responses indicated that 5.0 percent of the respondents strongly agreed to the statement, while 52.0 percent of them agreed, though 28.0 percent of them were neutral while 8.0 percent and 7.0 percent of them disagreed strongly and disagreed to the statement respectively. These findings implied that the County utilizes the IFMIS in running accounts department.

Finally, the respondents were asked whether sharing of flash disks, passwords and compact disks and opening of emails without scanning by the end users possess security risks. The distribution of the responses indicated that 26.0 percent of the respondents strongly agreed to the statement, while 53.0 percent of them agreed though 21.0 percent of them were neutral. Likewise of the respondents disagreed or strongly disagreed to the statement respectively. These findings implied that sharing of passwords, flash disks, compact disks, and open emails without scanning by the end users possess security risks.

Further, respondents were questioned whether sites containing suspicious links compromised organizations' security system and exposed them to various security dangers, 20.0 percent of the respondents strongly agreed, while 41.0 percent of the respondents agreed on the statement, but 10.0 percent of the respondents were neutral while 20.0 percent disagreed, 20.0 strongly disagreed. This implied that majority agreed that websites that contain suspicious links compromises the organizations security system and expose them to various security threats.

Table 4.1: Effect of Security Component on IFMIS Accountability in TransNzoia County

Statements	SA	A	N	D	SD	MEAN	STD DEV
IFMIS is protected by firewalls	30.0	37.0	18.0	10.0	5.0	3.944	0.912
IFMIS is protected by authenticated software	32.0	16.0	29.0	16.0	8.0	3.617	0.833
IFMIS is protected by anti-virus	20.0	42.0	34.0	4.0	0	3.448	0.698
The County utilizes the IFMIS in running accounts department	5.0	52.0	28.0	7.0	8.0	3.561	0.654
Sharing of flash disks, passwords and compact disks and opening of emails without scanning by the end users possess security risks	26.0	53.0	21.0	0	0	4.127	0.511
Sites that contain suspicious links compromised the organizations security system and exposed them to various security threats	20	41.0	10.0	20.0	20.0	3.696	0.676

4.2 Effect of IFMIS Accountability in Transnzoia County

The study sought to determine the effect of IFMIS Accountability in Transnzoia County. The findings are presented in a five point Likert scale where SA=Strongly Agree, A=Agree, N=Neutral, D=Disagree, SD=Strongly Disagree and T=Total. From table 4.2 below, the respondents when asked whether the technical staffs were able to configure and customize IFMIS System. The distribution of results showed that 37.0 percent of the respondents strongly agreed, 38.0 percent of them agreed, 2.0 percent of the respondents were neutral, 15.0 percent disagreed while 8.0 percent of them strongly disagreed. These findings implied that the technical staff is able to configure and customize IFMIS System.

The respondents asked whether the technical staff is able to trouble shoot and maintain the IFMIS System. The distribution of the responses indicated that 46.0 percent strongly agreed to the statement while 37.0 percent of them agreed and 3.0 percent of them were neutral, though 8.0 percent of them disagreed but 5.0 percent of them strongly disagreed to the statement. These findings implied that the technical staff is able to trouble shoot and maintain the IFMIS System. The respondents were also asked whether the County involves hired technical team with technical knowledge for the operation of IFMIS system. The distribution of the responses indicated that 39.0 percent strongly agreed to the statement, while 41.0 percent of them agreed, but 4.0 percent of them were neutral, and 8.0 percent of them disagreed while 11.0 percent strongly disagreed to the statement. These findings implied the County involves hired technical team with technical knowledge for the operation of IFMIS system.

The respondents were further asked whether technical staff offers trainings and orientation to other staffs in other departments within the County on IFMIS System application. The distribution of the responses indicated that 31.0 percent strongly agreed to the statement, while 52.0 percent of them agreed, but 6.0 percent of them were neutral while 9.0 percent and 2.0 percent of them disagreed strongly and disagreed to the statement respectively. These findings implied that technical staff offers trainings and orientation to other staffs in other departments within the County on IFMIS System application. The respondents when asked whether technical staff understand all types of infrastructure-hardware and software that runs the IFMIS System. The distribution of the responses showed that 29.0 percent strongly agreed to the statement, while 43.0 percent of them agreed, but 4.0 percent of them were neutral, though 14.0 percent of them disagreed while 7.0 percent of them strongly disagreed to the statement respectively. These findings implied that technical staff understands all types of infrastructure-hardware and software- that runs the IFMIS System.

The respondents were further asked whether technical staff fulfill end user needs. The distribution of the responses indicated that 30.0 percent strongly agreed to the statement, while 52.0 percent of them agreed, but 9.0 percent of them were neutral while 7.0 percent and 2.0 percent of them disagreed strongly and disagreed to the statement respectively. These findings implied that technical staff fulfils end user needs. The respondents when asked whether technical team have knowledge on IFMIS system Modifications as well on security setup. The distribution of the responses indicated that 29.0 percent strongly agreed to the statement, while 51.0 percent of them agreed, but 6.0 percent of them were neutral while 7.0 percent and 7.0 percent of them disagreed strongly and disagreed to the statement respectively. These findings implied that technical team have knowledge on IFMIS system Modifications as well on security setup.

Table 4.2: Effect of IFMIS Accountability in TransNzoia County

Statements	SA	A	N	D	SD	MEAN	STD DEV
The technical staff are able to configure and customize IFMIS System	37.0	38.0	2.0	15.0	8.0	4.411	0.511
The technical staff are able to trouble shoot and maintain the IFMIS System	46.0	37.0	3.0	8.0	5.0	4.326	0.658
The County involves hired technical team with technical knowledge for the operation of IFMIS system	39.0	41.0	4.0	8.0	11.0	3.178	0.921
Technical staff offers trainings and orientation to other staffs in other departments within the County on IFMIS System application	31.0	52.0	6.0	9.0	2.0	3.922	0.883
Technical staff understand all types of infrastructure-hardware and software- that runs the IFMIS System	29.0	43.0	4.0	14.0	10.0	3.414	0.544
Technical staff fulfill end user needs	30.0	52.0	9.0	7.0	2.0	3.557	0.648
Technical team have knowledge on IFMIS system Modifications as well on security setup	29.0	51.0	6.0	7.0	7.0	3.032	0.611
AGREGATE							

4.3 Diagnostic Tests

Prior to conducting inferential statistics, a number of diagnostic tests were checked. This was aimed at ensuring that the study data was not biased, which would result to inaccurate estimations. The tests included: multicollinearity, normality, and auto-correlation and linearity tests.

4.3.1 Multicollinearity Test

Multicollinearity is the occurrence of high interrelations among two or more interdependent variables in a multiple regression model. The test is used to check whether there is correlation among independent variables which results in less reliable statistical inferences. Therefore, the purpose of using multicollinearity test was to safeguard the study from using independent variables that were not correlated or repetitive when building multiple regression models that use two or more variables.

The study tested multicollinearity between independent variables using VIF. According to (Field, 2009), multi-collinearity is said to exist if there is a strong correlation between two or more independent variables in a model. The results indicate that all the variables had VIF values less than 10 and tolerance levels more than 0.1 implying that there was no multicollinearity among the independent variables. The results are shown in Table 4.3.

Table 4.3: Multicollinearity test using VIF

Variables	Tolerance	VIF
Security Component	.551	1.816

4.3.2 Normality Test

Normality test is used to determine whether sample data has been drawn from a normally distributed population (within some tolerance). Normality is important for data since it provide simple summaries about the sample and the measures. Measures of the central tendency and dispersion are used to describe the quantitative data (Anaesth, 2019). Normality of data was tested using the Shapiro-Wilk test. The rule of thumb is that when the P value (Sig) is greater than 0.05, the null hypothesis of normal distribution is not rejected. The findings (Table 4.4) indicate that all the variables had P values (Sig) greater than 0.05 implying that the data was normally distributed.

Table 4.4: Normality Test using Shapiro-Wilk

Variables	Statistic	df	Sig.
Accountability in Transnzoia County Government	0.966	240	.112
Security components	0.906	240	.077

4.3.3 Auto-correlation Test

Auto-correlation refers to the degree of correlation of the same variables between two successive time intervals. It measures how the lagged/protected version of the value of a variable is related to the original version of it in a time series (Scott, 2020). The test of auto-correlation was done using the Durbin-Watson test. This was done to check that the residuals of the model are not correlated since independence of the residuals is one of the basic hypotheses of regression analysis. Durbin Watson test reports a test statistic, with a value from 0 to 4, where; 2 is no autocorrelation, 0 to <2 is positive autocorrelation, >2 to 4 is negative autocorrelation. The rule is that test statistic values in the range of 1.5 to 2.5 are relatively normal, while values outside of this range could be cause for concern. The results (Table 4.5) indicate a Durbin-Watson value of 1.891 implying that the residuals were not auto-correlated.

Table 4.5: Durbin-Watson test of autocorrelation

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.652a	0.426	0.417	0.36774	1.891

a. Predictors: (Constant), X4

b. Dependent Variable: Y

4.4 Correlation Analysis

This section provides results on the relationship between the independent and dependent variables. the results indicate that security components [X4] had a positive and significant relationship with accountability in TransNzoia County Government ($r = .491$, $p = 0.000 < 0.05$). This implies that both security components and accountability in TransNzoia County Government move in the same direction. As such, an increase in security components is accompanied by accountability in TransNzoia County Government. Moss, Sharpley and Wilson (2014) asserted that security components was critical in determining accountability.

Table 4.6: Correlation Matrix; Integrated Financial Management Information Systems on Accountability in TransNzoia County

		Y	X1	X2	X3	X4
Y	Pearson Correlation	1				
	Sig. (2-tailed)					
X4	Pearson Correlation	.491**	.424**	.520**	.651**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	240	240	240	240	240

** Correlation is significant at the 0.01 level (2-tailed).

4.5 Multiple Regression Analysis without Moderation

Having separately established the effect of each independent variable on dependent variable, it was imperative to determine the combined effect of all the independent variables on Accountability in TransNzoia County Government. A multiple regression model was therefore, used to establish the effect of Integrated Financial Management Information Systems on Accountability in TransNzoia County Government.

The results (Table 4.7) indicate that all the independent variables jointly explain 43% ($R^2 = .426$) of the total variations in the Accountability in TransNzoia County Government. An F statistic of 52.597 and reported P value of $0.000 < 0.05$ revealed that the proposed model was significant (good fit) in predicting the dependent variable. This means that Integrated Financial Management Information Systems are significant predictors of the on accountability in TransNzoia County Government.

The findings further indicate that management skills ($\beta_2 = .327$, $P = .000$); technological skills ($\beta_3 = .339$, $P = .000$); and security components ($\beta_4 = .127$, $P = .041$) had a positive and significant effect on accountability in TransNzoia county. However, ICT infrastructure was found to have no significant effect on accountability in TransNzoia County Government ($P = .675 > 0.05$). Based on the coefficients (β), when all the independent variables are combined, technological skills best explains accountability in TransNzoia County Government, followed by management skills, followed by security components and lastly ICT infrastructure.

Model without moderation

$$Y = 0.858 + .339X_3$$

Table 4.7: Multiple Regression Model without moderation

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.858	.251		3.416	.001
	X4	.127	.062	.124	2.050	.041
	R Squared	.426				
	Adj. R Squared	.417				
	F statistic	52.597				
	P value	.000				

a Dependent Variable: Y

The fourth null hypothesis (H_{04}) predicted that security components did not have significant relationship with the accountability in TransNzoia County Government. A p value of 0.000 (Table 4.6) was less than 0.05 implying rejection of the null hypothesis in favour of the alternative. Therefore, security components had a significant relationship with accountability in TransNzoia County Government.

5. CONCLUSION AND RECOMMENDATIONS

Based on the findings the study concluded the following as follows; the fourth null hypothesis (H_{04}) predicted that security components did not have significant relationship with the accountability in TransNzoia County Government. A p value of 0.000 was less than 0.05 implying rejection of the null hypothesis in favours of the alternative. Therefore, security components had a significant relationship with accountability in TransNzoia County Government. Based on the findings, the researcher recommended the following: The top management and the staff should be willing and committed to change in the use of technology, strengthen the use of complex systems such as IFMIS, and achieve their public sector objectives through technical assistance and urgent maintenance, frequent updates and reliable service.

REFERENCES

- [1] Ameen, A. A., & Ahmad, K. (2011, November). The role of Finance Information Systems in anti-financial corruptions: A theoretical review. In *Research and Innovation in Information Systems (ICRIIS), 2011 International Conference on* (pp. 1-6). IEEE.
- [2] Arnety, N. M., Ujunju, M. O., & Wepukhulu, R. (2013). Effects of Business Process Re-engineering on Implementation of Financial Management Systems: A Case of Masinde Muliro University of Science and Technology. *Research Journal of Finance and Accounting*, 4(12), 90-96.
- [3] Bankole FO, Osei-Bryson KM and Brown I (2015a). The Impact of ICT Infrastructure and Complementary Factors on Intra-Africa Trade. *Information Technology for Development*, 21(1), 12-28.
- [4] Bednar, M. K. (2012). Watchdog or Lapdog? A behavioral view of the media as a corporate governance mechanisms. *Academy of Management Journal*, 55(1), 131-150
- [5] Bovens, M.A.P. 2005. Public Accountability. In *The Oxford Handbook of Public Management*, edited by E. Ferlie, L. Lynne and C. Pollitt. Oxford: Oxford University Press.

- [6] Chepkemai, P., & Njeru, A. (2017). Effect of ICT infrastructure on audit trail completeness in Kenyan county governments. *Journal of Public Financial Management*, 15(3), 214-229.
- [7] Davenport, T., H., (2000). *Mission Critical: Realizing the Promise of Enterprise Systems*, Harvard Business School Press, Boston, MA.
- [8] DeLone, W. H., & McLean, E. R. (2016). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 32(4), 61-88. Gilani N., S., (2012). *Vision of information technology*, Kadoos publisher.
- [9] Haque, M. Shamsul. (2000). Significance of accountability under the new approach to public governance. *International Review of Administrative Sciences* 66(1): 599-617.
- [10] Hendriks, C. J. (2019). Information systems and public sector accountability: The role of IFMIS in developing countries. *Government Information Quarterly*, 36(4), 101385. Humphreys, E. (2009). Implementing the ISO/IEC 27001—Information Security Management System Standard. *ISACA Journal*, 4.
- [11] Kessler, K., Hettich, N., Parsons, C., Richardson, C., & Triana, A. (2011). A Framework for Assessing Privacy Readiness of e-Government. *iGovernment*, 21.
- [12] Kothari, C., R., (2004). *Research Methodology: Methods and Techniques*. New Delhi, India: New Age International Publishers.
- [13] Kamau, L. W., & Otieno, G. A. (2019). Determinants of financial reporting accuracy in Kenyan county governments. *International Journal of Economics, Commerce and Management*, 7(2), 340-355.
- [14] Karanja, J. G., & Ng'ang'a, P. (2019). Implementation challenges of integrated financial management information systems in Kenyan county governments. *International Journal of Economics, Commerce and Management*, 7(2), 340-355.
- [15] Kibet, L. K. (2017). Effect of information communication technology infrastructure on implementation of integrated financial management information system in county governments in Kenya. *International Journal of Information Technology and Business Management*, 58(1), 48-53.
- [16] Kimani, N. (2016). Influence of ICT infrastructure on integrated financial management information system implementation in Kenyan county governments. *International Academic Journal of Information Systems and Technology*, 2(1), 1-18.
- [17] Kiptoo, J. K., & Mwirungi, F. M. (2018). Factors influencing effective implementation of integrated financial management information systems in county governments in Kenya. *International Journal of Management and Commerce Innovations*, 6(1), 1285-1293.
- [18] Laudon, K., C., & Laudon, J., P., (2006). *Management Information Systems (10th ed.)*. (Pearson, Ed.) Upper Saddle River, NJ, USA: Prentice Hall.
- [19] Laudon, K., C., Laudon, J., P., (2009). *Management Information Systems: Managing the digital Firm*. (11 ed.). Prentice Hall/CourseSmart. p.164
- [20] Lucas, H., C., (2007). "Research Methods in Information Technology." Lecture in BMGT 808B, University of Maryland, Spring (2007).
- [21] Makatiani, W. (2012). *Information Intelligence and Analytics*. Retrieved June 14, 2012,
- [22] Mohammed A., (2001). The Impact of Integrated Financial Management System on Economic Development: The Case of Ghana, M. A. *Graduate School of International Studies*, Korea University
- [23] Mohammad, S. S., & Awwad, M. (2018). The impact of system quality, information quality, and service quality on user satisfaction in e-government systems. *International Journal of Information Management*, 38(1), 1-13.
- [24] Millar, Michelle & David McKevitt. (2000). Accountability and performance measurement: An assessment of the Irish health care system. *International Review of Administrative Sciences* 66 (1):285-296.

- [25] Muigai, R. G., & Gitau, S. N. (2018). Effect of ICT capabilities on implementation of integrated financial management information system in Kenya government ministries. *Strategic Journal of Business & Change Management*, 5(1), 1078-1115.
- [26] Mutui, S. K., & Wanyoike, D. M. (2019). Influence of integrated financial management information system on financial performance of county governments in Kenya. *International Journal of Economics, Commerce and Management*, 7(5), 567-583.
- [27] Njihia, E., & Makau, G. (2019). ICT infrastructure and implementation of integrated financial management information system in county governments of Kenya. *International Academic Journal of Information Systems and Technology*, 2(1), 41-58.
- [28] Rasht. Re-Engineering, From Modular, to Full Cycle End-To-End Processes, Strategic Plan 2011-2013 *Kenya Gazette Supplement Acts*, 2012
- [29] Rai, A., Patnayakuni, R., & Seth, N. (2019). Firm performance impacts of digital transformation: The role of big data, AI, and digital platforms. *Information Systems Research*, 30(3), 838-860.
- [30] Seddon, P. B., & Kiew, M. Y. (2015). A partial test and development of the DeLone and McLean model of IS success. *Australian Journal of Information Systems*, 22, 1-21.
- [31] Turel, O., & Serenko, A. (2016). Satisfaction with information technology: A meta-analytic review. *Journal of Information Systems*, 30(4), 118-140.
- [32] Wang, W., & Liao, Z. (2019). Examining the effects of system and information quality on user satisfaction: A test of the DeLone and McLean IS success model in the context of cloud computing. *Information & Management*, 56(6), 635-650.
- [33] Yilmaz, S., Beris, Y. and Serrano-Berthet, R. (2008). Local Government Discretion and Accountability: A diagnostic Framework for Local Governance. Local Governance Accountability Series, Paper No. 113