INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS

ISSN(print): 2643-9840, ISSN(online): 2643-9875

Volume 08 Issue 03 March 2025

DOI: 10.47191/ijmra/v8-i03-42, Impact Factor: 8.266

Page No. 1278-1288

An Assessment of the Effect of Information Security Management System on Organisational Performance

Kwakye Agyapong, PhD[1], Isaac Boakye[2]

[1]Metropolitan Consulting Group

[2]Accra Institute of Technology

ABSTRACT: This study examines the effect of an Information Security Management System (ISMS) on organizational performance in a Small and Medium Business (SMB), with a focus on Red Mango Ltd. The study employed a correlational survey design to assess the relationship between ISMS implementation and organizational performance. Primary data was collected from 44 respondents, including management and staff, through structured questionnaires. The convenience sampling technique was used for respondent selection, and data analysis was conducted using the Statistical Package for Social Sciences (SPSS) version 25. Correlation and regression analyses were applied to determine the relationship and effect of ISMS on organizational performance. Findings revealed that ISMS is well-implemented at Red Mango Ltd, with clear policies, structured roles and responsibilities, and comprehensive employee training on security measures. Employees are well-informed about acceptable usage of information security systems, and security incidents are promptly reported. However, several challenges hinder ISMS implementation, including leadership issues, technical system difficulties, personnel constraints, and financial limitations. Despite these challenges, ISMS adoption has led to significant benefits, including regulatory compliance, optimized business processes, cost savings, improved information security awareness, enhanced company reputation, and increased productivity. The study further established a strong positive correlation between ISMS implementation and organizational performance at Red Mango Ltd. Regression analysis indicated that a unit increase in ISMS adoption results in a 0.495 increase in organizational performance, confirming its significant impact. The study concludes that effective ISMS implementation enhances security, improves operational efficiency, and contributes to overall business success. Organizations are encouraged to address implementation challenges through leadership commitment, technical capacity building, and financial investment to fully realize ISMS benefits.

KEYWORDS: Information Security Management System, ISMS, Organizational Performance, Small and Medium Business, Red Mango Ltd

INTRODUCTION

Technological innovations are changing methods and strategies adopted in business management. Businesses have adopted digital storage of data, which provides benefits such as ease of access and management as compared to the manual and physical data storage (Azeez & Yaakub, 2019). Other benefits associated with electronic data management include fast manipulation of data, vast storage space, eased accessibility of information, and eased sharing of the information (Jalagat & Al-Habsi, 2017). Data assets have evolved significantly from a single source to broad data exchange across the web, involving various organisations. This type of data is addressed by an assortment of media alluded to as "new technology forces" and is comprised of cloud computing, social media, and big data (Al-Rashdi, Dick & Storey, 2017).

However, uses of technology in business exposes the business to cybercrimes. It is vulnerable to both internal and external breach of information, and when that occurs, private and personal data reaches competitors, hackers falsify the data and that could lead to the downfall of the company (Azeez and Yaakub, 2019). Media Foundation for West Africa (2017) investigated the IT climate in Ghana's public and private sectors and reported that current inner and outer control measures are insufficient to recognize and forestall the attacks against them. The reports further elaborated that absence of a cybersecurity awareness culture is part of the likelihood of these technology-driven attacks to succeed. The Confidentiality, Integrity and Availability (CIA) of data are compromised after a breach. Therefore, there is the need to secure organizational data from manipulation by unauthorized users (Jain & Chawla, 2020).

An Assessment of the Effect of Information Security Management System on Organisational Performance

Nowadays, most businesses can process their information faster than before thanks to technological advancement, and information is frequently viewed as the backbone without which a company cannot function (Jalagat & Al-Habsi, 2017). Information Technology dynamics and developments have made it vital for business entities to keep their indispensable data resources from being exploited by unauthorised users (Jain and Chawla, 2020). Ernst & Young, (2010) indicated that organisations investment in information security has increased over the years.

Data security is accomplished by carrying out suitable control measures, including guidelines, procedures, methodology, hierarchical designs, as well as roles of equipment and their applications (Jain & Chawla, 2020). These measures should be implemented and fundamentally inspected and further developed where important to guarantee that the business' security targets are met (Jain & Chawla, 2020). Businesses adopt and implement Information Security Management System (ISMS) in their quest to enhance security of their information. ISMS is a framework developed at the core of the operations that enables the operator to manage, monitor, review, and improve the information security practice universally from one point (Irwin, 2019). It entails strategies, techniques, and controls that are designed to enhance privacy, accuracy, and accessibility of the data to the authorized personnel only.

ISMS integrate the use of International Standards Organization (ISO) 27001 (ISO 27001), which is a framework designed to track the operations of an organization by providing several entities that would require provision of information (Irwin, 2019). The analysis of the collected data provides the needed information at the security levels of the firm, outlining the risks associated and areas that would need improvement of the safety measures. Sing and Gupta (2019) explained that senior management backing is essential to the organisation's information security management effectiveness. Susanto, Almunawar, and Tuan (2011) emphasised the role of ISMS in an organisation by explaining that due to the growing business competitiveness, it is of paramount importance for organizations to use Information Security Management System (ISMS) as they are faced with data theft and spying on business strategy, which negatively affects organizational performance. Hangbae (2012) also opined that ISMS's role is to efficiently build and consistently oversee the measures for securing one of the most important assets of the company, information.

Statement of the Problem

Attaining optimal organisational performance has always been the focal point of company's operations (Jalagat, 2017). To achieve organisational performance, information has been recognised as a valuable corporate asset that enables organisations to add to their products and services, reduce cost and meet customers need (Collins and Lanz, 2019). Given the integral role of information technology in today's business management, information security has become a key component in achieving a competitive advantage. As organizations growth rate increases, security at the management level becomes more challenging (Chang and Ho, 2006).

Companies across the world, including Red Mango Limited, must deal with the challenge of achieving Confidentiality, Integrity and Availability (CIA) of their information. Indeed, Studies have shown that several organisations have run into loss or collapsed due to information mismanagement or security breach (Kandel and Ndungu, 2015). Globally, it has been estimated that the world business environment loses about billions of dollars annually due to information breaches and this have great impact on organizational performance (Gutta, 2019). Based on this, it has become imperative for organizations to use standardised and proofed methods to manage efficiently their information assets.

Research Aim and Objectives

The main objective of the study will be assessing the effect of Information Security Management System on organizational performance for a Small and Medium Business (SMB).

To achieve this aim, the following objectives will be set:

1. To assess the perception staffs of Red Mango LTD have on Information Security Management System.
2. To examine the challenges faced by Red Mango LTD in implementing Information Security Management System.
3. To assess the effect of Information Security Management System on organization performance of Red Mango LTD.

2.2 THEORETICAL LITERATURE

2.2.1 Socio-Technical Theory

A socio-technical system is founded and defined upon two categories: the technical and the social. Both groups are equally crucial to information security (Iivari, & Hirschheim., 1996.). The risk-investment approach towards an ISS is viewed as a socio-technical one because both technological and social considerations are essential to its success. Several studies revealed that organizations experience information security incidents or cybersecurity risks predominantly due to human factors (Bagchi & Udo, 2003; Aitoro, 2008). These studies have provided various approaches and models, responding to the ever-increasing demand to understand human factors (Hayden, 2009). They have drawn from various theories across various fields such as

psychology, including occupational psychology (Blackler & Brown, 1986), sociology, including socio-technical theory (Palvia, Sharma & Conrath, 2001), and criminology, particularly deterrence theory amongst others.

Each has attempted to explain the role of human factors in information security risks and incidents. All these techniques are beneficial to the identification and modelling of human factors. However, few have presented a model explaining how people roles resulted from forces behind direct and indirect human factors and how organizations could effectively address the driving and resisting forces to change undesired situations to an ideal situation (D'Arcy, Hovav, & Galletta, 2009). This is a challenge since human factors are a subjective matter and require socio-technical systems theory and practice to be dealt with comprehensively. However, it is evident that ISSs comprise a blend of people who work within a technological process (Kun & Bray, 2010). This integration and co-ordination of an ISS has both social and technical views, creating a socio-technical nature in those forces involved (Beatson, 2011).

This marriage of people and process is quite similar to that presented by the Tavistock Institute for the British coal mining industry, where new machines were supposed to be run by people who were required to learn new technical skills (Tricker, 2013). This combination of technology and humans is complex and delicate. The complexity arises from the number of systems and skills involved and the delicacy from the dynamic relationship among these systems within the organisation (Appelbaum, 1997). Many researchers therefore believe that an ISS serves a deep and interdependent socio-technical function (Kun & Bray, 2010).

Herzberg's Two-Factor Theory

According to Herzberg's two-factor theory, Organisational performance implies motivating factors and the factors that cause complaints are denoted as hygiene factors (Kong, Jung, Lee & Yeon, 2015). Other motivational variables involve senses of accomplishment, solidity, work and leadership while other hygiene elements encompass policy management, direction, mutual relationships, working environment and wages (Herzberg, Mauner & Snyderman, 2009; Herzberg, 1996). The work itself, methods individuals utilize in working and a person's want to develop relate to motivational variables. Hygiene variables however are related to one's drive to circumvent troubles and the means individuals use to carry out their function and comprised of variables outside of people's work. Therefore, organisation's performance is dependent on both variables as motivation factors are the ingredient for good performance whereas hygiene elements characterise bad performance (Herzberg, Mauner & Snyderman, 2009). The two types of elements are not contracting concepts but two distinct points of view. As a result, they must be adequately joined. If this theory's validity is acknowledged, an employer ought to grant due consideration to making strides at improving work substance to oversee the performance of the organisation. (Kong, Jung, Lee & Yeon, 2015). Other research, on the other hand, have shown that Herzberg's two-factor theory has flaws by giving numerous instances that indicate that motivational and hygienic variables are not stable and may alter depending on the individual, work, time, or encompassing circumstances. (Amabile, 2012).

Information Security and Performance

Since data has become a key source of metric that inform the decision-making process, its safety and reliability is paramount for organizations. Diesch et al. (2020) affirm that most enterprises, such as banks, extensively rely on data to perform and remain competitive. This situation is attributed to the fact that most operations have become digitized, which has enhanced convenience but also introduced some risks. Concerning the latter, Malatji et al. (2020) acknowledge that the enterprise security attacks are growing continuously, and perpetrators are constantly advancing preferred methods. This occurrence has prompted enterprises to undertake necessary information security measures to maintain desired performance levels. When an organization has implemented reliable information security, it can protect its source of a competitive advantage and remain ahead of rivals. Additionally, a data breach can disrupt operations because a company might discontinue all activities until they identify and resolve all risks. Hence, information security is an integral component of business activities and influences performance levels.

Kehinde and Yusuf (2012) studied the position of ISMS as a stimulus for organisational success in the twenty-first century by questioning sixty staff members of three banks in Nigeria. ISMS is critical to an organisation in the twenty-first century because without properly managed information system, success and growth cannot be attained.

In addition, in Jordan, Khresat (2015) investigated the correlation between ISMS and the performance of an organisation. The population of the study covered all telecommunication organizations in the Amman city. The study found that the staffs in Jordanian telecommunication companies have positive behavior towards ISMS. The outcome of the study detected that there is a statistically important relationship between ISMS and organizational performance in telecommunication firms in Jordan.

Agu, Ugwu, and Igwegbe, (2017) examined the impact of ISMS on the performance of 7up organisation with 297 employees responding to questionnaires. Their research found that information asset is worthless except if used by the right administration work force. They concluded that without an appropriately constructed ISMS, the original data is generally futile and added that

the low degree of interest and backing for ISMS implementation in the company has reduced its impact on the company's productivity.

METHODOLOGY

Research Approach

Positivism was the adopted research philosophy, an approach which is commonly used to quantitatively evaluate predictive hypotheses, where practical correlations are obtained between descriptive factors or independent variable, and results or dependent variables (Park, Konge and Artino, 2020). Additionally, the study used deductive thinking which broadens understanding and relies on logical reasoning (Bansal et al. 2018). The research used a quantitative approach with the aid of questionnaires in collecting primary data. This approach aided in collecting details that were transformed into reliable data (Bansal et al. 2018). Aliaga and Gunderson (2002) depicted quantitative investigation approach as an examination into a social issue by clarifying situations through the gathering of a numerical information and analysing them scientifically

Research Design

A research design represents the blueprint that guides the study in collecting required information to solve the research problem and its objectives (Tustin, Lighthelm, Martins & Van Wyk, 2005). The researcher used closed end questionnaires survey method to collect original data from sampled population (Polit & Hungler, 1993).

The study used a correlational survey design to collect data, test and measure statistical relationship (how relevant) between variables without affecting them (Seeram, 2019), based on a null hypothesis (Ho) that there is no relationship between the two variables under study, ISMS and performance for a Small and Medium Business (SMB) organisation, and an alternate hypothesis (Ha) that there is a connection. This design method was appropriate to decide on the outcome based on the data obtained from survey. The research used regression analysis to assess the strength and direction of correlations values obtained between the two variables.

Population

According to Malhotra (2007) the population of a research is the collection of elements that possess the information being sought after by the researcher and about which inferences could be drawn. The target population of interest for the study were management and staff of Red Mango LTD.There are four (4) departments with a total population of forty-four (44). Males constitute seventy-five percent (75%) and females represent twenty-five percent (25%).

Sample Size

Sample size can be defined as the proportion of the sample that is representative enough of theentire population and whose findings can be generalized to the entire group (Hayes, 2008; Salkind, 2011). The analysis of results was done based on data collected from twenty-two (22) respondents.

Sampling Technique and Procedure

The study employed convenience sampling technique in selecting respondents. Convenience sampling is a non-probability sampling technique used to create sample as per ease of access, readiness to be a part of the sample, availability at a given time slot of the respondents (Bhat, 2018). Management and staff of Red Mango being the targeted population for this study, questionnaires were sent to everyone using google form. The researcher was unable to have physical contact with most of the respondents due to social distancing protocols in place during the period.

Data Collection Instrumentation

The main instruments for the study were structured questionnaires. A questionnaire is a technique for collecting data in which respondents are required to answer the same set of questions in a predetermined order (Zikmund, Babin, Carr & Griffin, 2010). Questionnaire was chosen because it helped the researcher to get the direct response and feedback from the respondents in a short period of time with low-cost effectiveness.

Validity of the Instruments

According to Collis and Hussey (2009), validity is known as the degree of precision with which a scale measures what it claims to calculate. Face validity entails selecting the appropriate instrument and soliciting the help of individuals who are skilled and experienced in the field, to determine if the measure accurately represents the definition. The questionnaires presented to respondents measured the required constructs, with anonymity an additional factor that prevented any restraints in collected information.

Reliability of the Instruments

Hayes (2008) opined that reliability refers to how much a research method achieves stable outcomes at disparate moments. This study used a test-retest procedure to ensure that the instrument used will repeat the same outcomes at various times. The reliability was calculated using Cronbach's alpha to obtain the internal consistency reliability coefficients. Hair, Ringle and Sarstedt (2010) recommended that instruments used in basic research have reliability value of about 0.70 or better to be acceptable to show internal consistency.

Data Analysis

The results were analysed in quantitative manner. The questionnaires used in the study helped the researcher to analyse results using Statistical Package for Social Sciences (SPSS) software. SPSS is the most widely used software package allowing several kinds of analysis, data conversion and output form that fully satisfied the objectives of this study (Stehlik-Barry, 2017). The objectives were analysed using frequency table, descriptive statistics, and regression analysis.

DATA ANALYSIS, RESULTS AND DISCUSSIONS

Reliability Analysis

Reliability of the questionnaire was evaluated through Cronbach's Alpha which measures the internal consistency. Cronbach's alpha was calculated by application of SPSS version 25 for reliability analysis. The range of values of the alpha coefficient is comprised between 0 and 1 and might be utilized to portray the reliability of variables from questionnaires at 5% degree of weight. The higher the coefficient, the greater the shared covariance of variables and presumably measure a similar notion. Cooper & Schindler (2008) have indicated 0.7 to be an acceptable reliability coefficient.

Table 4.1 Reliability Coefficient

Scale	No ofitems	Cronbach's Alpha
Perception staffs have on ISMS	11	0.917
Challenges facing Red Mango LTD in implementing ISMS	6	0.875
Benefits associated with the adoption and implementation of ISMS at Red Mango LTD	15	0.913
Organizational performance	15	0.913

Source: *Field Survey (2025)*

r>0.70= very strong reliability; 0.50 ≤ r<0.70 = strong reliability; 0.20≤ r ≤ 0.50 = moderate reliability; 0.10 ≤ r < 0.20 = weak reliability; r<0.10 = none/ negative reliability.

Table 4.1 shows the reliability coefficient for perception staffs of Red Mango LTD have on Information Security Management System (α=0.913), challenges facing Red Mango LTD in implementing InformationSecurity Management System (α=0.875), Benefits associated with the adoption and implementation of ISMS at Red Mango LTD (α=0.913) and finally the effect of Information Security Management System on organizational performance of Red Mango LTD (α=0.913). This illustrates that all the scales (11, 6, 15 and 15 respectively) were reliable as their reliability values exceeded the prescribed threshold of 0.70 (Mugenda & Mugenda, 2009).

Perception staffs of Red Mango LTD have on Information SecurityManagement System

The researcher assessed the perception staffs of Red Mango LTD have on Information SecurityManagement System with a five (5) point Likert scale with 1.0-1.49 representing "Strongly disagree", 1.50-2.49 for "Disagree", 2.50-3-49 equivalent to "Neutral", 3.50-4.49 for "Agree" and 4.50-5.0 representing "Strongly Agree". This has been chronologically expressed below.

Table 4.3: Descriptive Statistics staffs perceptions of ISMS at Red Mango Ltd.

	N	Mean	Std. Deviation
Security Policy			
Role and responsibilities for Information Security Management System (ISMS) in our organization are well defined	22	4.00	1.024
We have a well-documented ISMS Policy	22	4.00	.926

All staff are given adequate and appropriate ISMS Education and Training	22	3.64	1.136
Staff are well informed as to what is acceptable and unacceptable usage of our information security systems	22	3.77	1.066
Organization Security			
Third party (outsider) access to our information systems requires approval by a senior manager	22	4.18	.907
Directors ensure staffs are given basic knowledge on organization security	22	4.05	.899
Despite being connected to public networks, our systems are adequately protected by our ISP security and firewalling systems	22	4.45	.800
Personnel Security			
Staff are aware that security incidents must be reported to management immediately	22	3.95	.844
Staff have been trained to always secure their computers when moving away from their workstations	22	4.05	.722
There is a formal disciplinary process for employees who have violated our security policies and processes	22	3.59	.959
Appropriate mechanisms are in place to authenticate users logging onto our systems	22	4.36	.848
Valid N (listwise)	22		

Source: *Field Survey (2025)*

Security Policy

With the statement "Role and responsibilities for Information Security Management System (ISMS) in our organization are well defined.". The responses to this statement had an average mean of 4.0 and this indicates that the respondents agreed that Role and responsibilities for Information Security Management System (ISMS) in Red Mango Limited are well defined. The second statement posed to them was "We have a well-documented ISMS Policy". The responses accorded to this statement had an average mean of 4.0. This simply means that the respondents agreed to the statement.

The study sought to ascertain whether the respondents agreed or disagreed to the statement that "All staff are given adequate and appropriate ISMS Education and Training". The mean of the responses accorded to this is 3.64 and this implies that the respondents agreed to the statement that all staff are given adequate and appropriate ISMS Education and Training. Again, the statement "Staff are well informed as to what is considered to be acceptable and unacceptable usage of our information security systems" was accorded with a mean value of 3.77 which also implies that respondents agreed to the statement that Staff are well informed as to what is acceptable and unacceptable usage of Red Mango Limited information security systems.

Organizational security

Again, the statement "Third party (outsider) access to our information systems requires approval by a senior manager". The mean for the responses to the statement was 4.18 and this shows that the respondents agreed to the statement that third party (outsider) access to Red Mango Limited information systems requires approval by a senior manager. The study again sought to ascertain whether the respondents agreed or disagreed to the statement that "Directors ensure staffs are given basic knowledge on organization security". The mean of the responses accorded to this was 4.05 and this implies that the respondents agreed to the statement. The average mean value for "Despite being connected to public networks, our systems are adequately protected by our ISP security and firewalling systems" was 4.45 which implies that respondents strongly agreed that despite being connected to public networks, Red Mango Limited systems are adequately protected by the company's ISP security and firewalling systems.

Personnel Security

Again, the statement "Staff are aware that security incidents must be reported to management immediately" had a mean value of 3.95 which implies that the respondents agreed that staffs are aware that security incidents must be reported to management immediately. Again, the statement "Staff have been trained to secure their computers at all times when moving away from their workstations". The mean for the responses to the statement was 4.05 and this shows that the respondents agreed to the statement that staff have been trained to always secure their computers when moving away from their workstations. The study

again sought to ascertain whether the respondents agreed or disagreed to the statement that "There is a formal disciplinary process for employees who have violated our security policies and processes". The mean of the responses accorded to this was 3.59 and this implies that the respondents agreed to the statement. Finally, the statement "appropriate mechanisms are in place to authenticate users logging onto our systems" had a mean value of 3.95 which implies that the respondents agreed that appropriate mechanisms are in place to authenticate users logging onto our systems.

It's emerged from the that role and responsibilities for Information Security Management System (ISMS) in Red Mango Limited organization are well defined, Red Mango Limited have a well-documented ISMS Policy, all staff are given adequate and appropriate ISMS Education and Training and staff are well informed as to what is considered to be acceptable and unacceptable usage of Red Mango Limited information security systems.

Finding again brought out to the known that third party (outsider) access to Red Mango Limited information systems requires approval by a senior manager, Directors ensure Red Mango Limited employees are given basic knowledge on organization security and, despite being connected to public networks, Red Mango Limited systems are adequately protected by Red Mango Limited ISP security and firewalling systems.

Findings again brought out to the known that employees of Red Mango Limited are aware that security incidents must be reported to management immediately, employees have been trained to always secure their computers when moving away from their workstations, there is a formal disciplinary process for employees who have violated our security policies and processes and also, appropriate mechanisms are in place at Red Mango Limited to authenticate users logging onto our systems.

The challenges facing Red Mango LTD in implementing InformationSecurity Management System

The researcher sought to examine the challenges facing Red Mango LTD in implementing InformationSecurity Management System with a five (5) point Likert scale with 1.0-1.49 representing "Strongly disagree", 1.50-2.49 for "Disagree", 2.50-3-49 for "Neutral", 3.50-4.49 being "Agree" and 4.50-5.0 representing "Strongly Agree". This has been chronologically expressed below.

Table 4.3: Descriptive Statistics challenges facing Red Mango Ltd

	N	Mean	Std. Deviation
Management process issues	22	1.7325	1.279
Organizational environment issues	22	2.6364	1.98915
Leadership issues	22	3.5727	1.90693
Technical system issues	22	4.2273	1.90067
Personnel issues	22	4.0000	1.71825
Financial issues	22	3.6364	1.61968
Valid N (listwise)	22		

Source: *Field Survey (2025)*

The respondents were asked if management process issues are one of the challenges faced by Red mango Limited in implementing information security management system. The responses to the statement had a mean value of 1.7325. This implies that the respondents disagreed to the statement. Again, the statement "Organizational environment issues". The responses to this statement had an average mean of 2.6364 and this indicates that the respondents neither agreed nor disagreed to the statement that Organizational environment issues is one of the challenges faced by Red mango Limited in implementing information security management system.

The next statement posed to them was "Leadership issues is one of the challenges faced by Red mango Limited in implementing information security management system". The responses accorded to this statement had an average mean of 3.5727. This simply means that the respondents agreed that Leadership issues is one of the challenges faced by Red mango Limited in implementing information security management system. The study sought to ascertain whether the respondents agreed whether technical system issues is one of the challenges faced by Red mango Limited in implementing information security management system. The average mean value of the responses accorded to this is 4.227 and this implies that the respondents agreed to the statement. Again, the statement "personnel issues is one of the challenges faced by Red mango Limited in implementing information security management system" had a mean value of 4.0000 which also implies that respondents agreed that Personnel issues is one of the challenges faced by Red mango Limited in implementing information security management system. Again, respondents were again asked if "Financial issues is one of the challenges faced by Red mango Limited in implementing information security management system". The responses to the statement had a mean value of 3.6364. This implies that the respondents agreed to

the statement that financial issues are one of the challenges faced by Red mango Limited in implementing information security management system.

Findings brought out to the known that respondent disagreed that management process issues is one of the challenges faced by Red mango Limited in implementing information security management system. It again emerged from the study that respondents neither agreed nor disagreed that organizational environment issues are one of the challenges faced by Red mango Limited in implementing information security management system.

However, the study revealed that leadership issues, technical system issues and personnel issues are one of the challenges faced by Red mango Limited in implementing information security management system. The study again brought out to the known that financial issues is one of the challenges faced by Red mango Limited in implementing information security management system.

The effect of Information Security Management System on organizational performance of Red Mango LTD

Corelation Analysis

The study sought to determine the relationship between Security Management System on organizational performance at Red Mango LTD.

Table 4.6: Correlations of ISMS on organizational performance

		ISMS	Performance
ISMS	Pearson Correlation	1	.681**
	Sig. (2-tailed)		.000
	N	22	22
Performance	Pearson Correlation	.681**	1
	Sig. (2-tailed)	.000	
	N	22	22

**. Correlation is significant at the 0.05 level (2-tailed).

Source: *Field Survey (2025)*

Table 4.4 detailed the Pearson Product Moment Correlation (PPMC) which was used to establish and test the relationship between Information Security Management System on organizational performance at Red Mango LTD was Pearson's Product Moment correlation. **(r)=** 0.681. This clearly indicates that there is a strong positive relationship between Information Security Management System on organizational performance at Red Mango LTD. Now as to whether the relationship significant can be seen from the significant 2 tailed tests. The significant 2-tailed was 0.000 which less than 0.05, this indicated that there is significant correlation between Information Security Management System on organizational performance at Red Mango LTD. Therefore, there is significant correlation between Information Security Management System on organizational performance at Red Mango LTD. In a nutshell, the correlation between Information Security Management System on organizational performance at Red Mango LTD is positive and a strong positive linear relationship.

Hypothesis

Decision Rule: If P>0.05 Accept Ho and Reject Ha

If P< 0.05 Reject Ho and Accept Ha

The significant 2-tailed value was 0.000 which less than 0.05, this indicated that there is a significant correlation between Security Management System on organizational performance at Red Mango LTD. Therefore, the alternate hypothesis was accepted which indicated that there is a significant relationship between Information Security Management System on organizational performance at Red Mango LTD and the null hypothesis which indicated that there is no significant relationship between Information Security Management System on organizational performance at Red Mango LTD was rejected.

Regression Analysis

A multiple regression analysis was conducted to test the effect of the independent variable on the dependent variable. The SPSS tool was applied to code, enter and compute the measurements of the multiple regressions for the study.

Table 4.7 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.681[a]	.464	.437	.38241

a. Predictors: (Constant), ISMS

Table 4.8 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.530	1	2.530	17.299	.000[b]
	Residual	2.925	20	.146		
	Total	5.455	21			

a. Dependent Variable: Performance

b. Predictors: (Constant), ISMS

Table 4.9 Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	1.969	.484		4.067	.001
	ISMS	.495	.119	.681	4.159	.000

a. Dependent Variable: Performance

Source: *Field Survey (2025)*

Model Summary

Coefficient of determination (R Square) explains the extent to which changes in the dependent variable can be explained by changes in the independent variables or the percentage of variation in the dependent variable (organizational performance) that is explained by the independent variable (Information Security Management System).

Table 4.7 above reveals R2 of 0.464 which implies that the independent variables studied explain only 46.40% of the variations in organizational performance at Red Mango Limited. This shows that 46.40% percent changes in organizational performance at Red Mango Limited could be accounted to changes in the independent variable (Information Security Management System System) used in the study. Consequently, this means that other factors not stated in this research explain 53.3% of the variations in organizational' performance at Red Mango Limited.

Analysis of Variance

From the findings the significance value (p- value) is 0.000 which is less than 0.05 thus the model is statistically significance in predicting how the independent variables affect organizational performance at Red Mango Limited. The calculated value at 5% level of significance was 17.299. Since the calculated value is greater than the critical value (17.299>0.000), this shows that the overall model was significant and the model can be used to predict the effect of Information Security Management System on organizational performance of Red Mango LTD.

Regression Coefficient

$Y = \beta_0 + \beta_1 X_1 \ldots\ldots + \varepsilon$

$Y = 1.969 + 0.495X \ldots + \varepsilon$

According to the regression equation established, taking all factors into account (the independent variables) at zero, organizational performance at Red Mango Limited will be 1.969. The data findings analyzed also show that taking all other independent variables at zero, a unit increase in the independent variable (Information Security Management System) will lead to 0.495 increase in organizational performance at Red Mango Limited. This implies that the independent variable contributes to organizational performance at Red Mango Limited. The findings also revealed that Information Security Management System positively influence organizational performance. This implies that a unit increase in Information Security Management System will lead to 0.495 increase in organizational performance. At 5% level of significance and 95% level of confidence, the independent variable (Information Security Management System) significantly influenced organizational performance.

CONCLUSION AND RECOMMENDATIONS

The main objective of the study is to assess the effect of Information Security Management System on organizational performance for a Small and Medium Business (SMB) using New Mango Limited as a study. Information is one of the key elements of productivity and thus, must be managed similarly as the human and monetary assets of the organisation. However, the quintessence of information as a key resource to the company is greater when driven by higher level than the bottom. The research revealed that management of Red Mango Limited reckon the importance of information systems in decision making, even though not sufficiently dedicated to improving upon it. The study showed that ISMS enable the employees of the organization to do their task adequately as they obtain data at the ideal time and can share it. Staff of Red Mango Limited do not need to gather

information physically for documentation, archiving and reviewing. Hence, blunder and redundancy are diminished, enabling them to provide decision-makers with high-quality information. ISMS therefore play an extraordinary part on the productivity of Red Mango's employees.

The following recommendation are made from the conclusion of the study, which ascertain that ISMS has a positive impact on organisational performance. The recommendations are made to help SMBs improve productivity by adopting the right information systems attitude using ISMS.

Findings from the regression analysis revealed that Information Security Management System positively influence organizational performance. It is therefore recommended that there should be proper handling and processing of information because it can decide the fate of the organization. This therefore means that if organizations use information system in their operation properly, they will be on the position to achieve their goals whereas the reverse could be fatal to the company.

Moreover, the correlation analysis also brought out to the known that there is a strong positive correlation between Information Security management System and Organizational performance at Red Mango Limited. It is therefore recommended that for an organization to be effective, information is as important resource as money, machinery, and manpower. It is essential for the survival of the enterprise hence to fulfil the needs of information the management of information system is critical for the prosperity of every business organization.

Furthermore, Managers need rapid access to information to make decisions about strategic, financial, marketing, and operational issues and they are successfully handling information and applying it when making decisions. They see information as asset, creation of information ethos is one part of ongoing process, and those companies which have successfully implemented change and created an information ethos have done so with the backing and leadership of the senior managers, and the CEO.

Additionally, ISMS helps to address technical problems and emergencies that may affect Red Mango Limited operations and, Red Mango Limited uses ISMS to help the organization to optimized operations within the organization because of clearly defined responsibilities and business process. The researcher therefore recommends that Managers need rapid access to information to make decisions about strategic, financial, marketing, and operational issues and they must successfully handle information and applied it when making decisions to improve upon the performance of the organization. It is recommended that management must see information as asset and see creation of information ethos as one part of ongoing process to help improve performance.

Findings again revealed that Information enables organization to make more accurate decisions. For this reason, the right amount of information at the right time is a key factor for every organization. Company managers must therefore take decisions, prepare plans, and control their company's activities using information.

REFERENCES

1) Abugabah, A., Sanzogni, L., & Poropat, A. (2012). The Impact of Information Systems onuser Performance: A critical review and theoretical model. Nathan, Brisbane, QLD 4111, Australia.
2) Al-Rashdi, Z., Dick, M., & Storey, I. (2017). Literature-based analysis of the influences of the new forces on isms: a conceptual framework. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December 2017, Edith Cowan University, Perth, Western Australia. (pp.116-124). This Conference Proceeding is posted at Research Online.https://ro.ecu.edu.au/ism/213
3) Amarachi, A.A., Okolie, S.O., & Ajeagbu, C. (2013). Information Security Management System: Emerging Issues and Prospect. *Journal of Computer Engineering (IOSR-JCE),*
4) Azeez, R.T., & Yaakub, K.B. (2019). The Effect of Management Information System on Organizational Performance: A Survey Study at Missan Oil Company in Iraq. *Journal of Global Scientific Research.* Vol 2, p 135-165
5) Bansal, P., Smith, W. and Vaara, E., 2018. New Ways of Seeing through Qualitative Research. *Academy of Management Journal*, 61(4), pp.1189-1195.
6) Bansal, Pratima & Smith, Wendy & Vaara, Eero. (2018). New Ways of Seeing through Qualitative Research. Academy of Management Journal. 61. 1189-1195. 10.5465/amj.2018.4004.
7) Bashroush, R., Akinyemi, I. and Schatz, D., 2020. SWOT analysis of information security management system ISO 27001. *International Journal of Services Operations and Informatics*, 10(4), p.305.
8) Bongiovanni, I., 2019. The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security*, 86, pp.350- 357.
9) Chang, S.E., & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, Vol 1
10) Collins, V. and Lanz, J., 2019. Managing Data as an Asset. *The CPA Journal*,.
11) Cooper, D. R., & Schindler, P. S. (2014). Business Research Methods 12th Edition. In Business Research Methods.

12) da Veiga, A. and Martins, N., 2015. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*,49, pp.162-176.
13) da Veiga, A. and Martins, N., 2017. Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70, pp.72-94.
14) da Veiga, A., Astakhova, L., Botha, A. and Herselman, M., 2020. Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, 92, p.101713.
15) Diesch, R., Pfaff, M. and Krcmar, H., 2020. A comprehensive model of information security factors for decision-makers. *Computers & Security*, 92, p.101747.
16) doi: 10.1097/ACM.0000000000003093
17) Dutton, J., 2020. *What Is An ISMS? 9 Reasons Why You Should Implement One - IT Governance UK Blog*. [online] IT Governance UK Blog. Available at: <https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one> [Accessed 28 Mai 2020].
18) Hangbae Chang, 2012. Is ISMS for financial organizations effective on their business? Mathematical and Computer Modelling, Volume 58, Issues 1–2,2013, Pages 79-84, ISSN 0895-7177, https://doi.org/10.1016/j.mcm.2012.07.018.
19) Hassan, N. and Ismail, Z., 2012. A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. *Procedia - Social and Behavioral Sciences*, 65, pp.1007-1012.
20) Irwin, L., 2019. *What Is An ISMS And Why Does Your Organisation Need One? - IT Governance Blog En*. [online] IT Governance Blog En. Available at: <https://www.itgovernance.eu/blog/en/what-is-an-isms-and-why-does-your-organisation-need-one> [Accessed 28 July 2020].
21) Jain, S. and Chawla, D., 2020. A Relative Study on Different Database Security Threats and their Security Techniques. *International Journal of Innovative Science and Research Technology*, 5(1), pp.794-199.
22) Jalagat, R. (2017). Reflecting Change in a Changing World: The Human and Spiritual Dimension. *European Business & Management*, 4(3-1): 1-5. doi: 10.11648/j.ebm.s.2018040301.11
23) Kandel, S., & Ndungu, M. (2015). Information Security Management in Organizations. An unpublished project work submitted to Centria AMMATTIKORKEAKOULU.
24) Malatji, M., Marnewick, A. and von Solms, S., 2020. Validation of a socio-technical management process for optimising cybersecurity practices. Computers & Security, 95, p.101846.