

Proposing a Model for Promoting the Performance of Information Flow in Organizations Using SISP Approach

Muneer Hazaa Alsurori^{1, *}, Juhana Salim², Khaled Ahmed Almasni³

¹Department of Mathematics & Computer Science, Faculty of Science, Ibb University, Ibb, Yemen

²Department of Information Science, Faculty of Information Science and Technology, University Kebangsaan Malaysia, Bangi, Malaysia

³Department of Statistics Science, National Institute of Administrative Sciences, Taiz, Yemen

Email address:

msurory@yahoo.com (M. H. Alsurori), js@ftsm.ukm.my (J. Salim), kalmasany@yahoo.com (K. A. Almasni)

*Corresponding author

To cite this article:

Muneer Hazaa Alsurori, Juhana Salim, Khaled Ahmed Almasni. Proposing a Model for Promoting the Performance of Information Flow in Organizations Using SISP Approach. *Internet of Things and Cloud Computing*. Vol. 5, No. 2, 2017, pp. 19-28.

doi: 10.11648/j.iotcc.20170502.11

Received: September 12, 2016; **Accepted:** March 27, 2017; **Published:** April 17, 2017

Abstract: This study aimed to develop and to validate a Strategic Information Systems Planning (SISP) model designed to improve the information flow performance by incorporating the antecedent factors into information technology components, information needs and security of information flow factors. The methodology was carried out in four phases; the theoretical study, the conceptual framework design, the survey design, the data analysis, and the model development and validation phase. Questionnaires were distributed to 350 employees at the Ministry of Higher Education and Scientific Research (MoHESR) and four (4) government universities in Yemen for data collection. Based on the correlation results, it was found that information technology components have significant relationship with information needs. Moreover, information technology components have a direct significant relationship with the security of information flow in the MoHESR and universities in Yemen and they have indirect influence through the information technology components on the security of information flow in the MoHESR and universities in Yemen. By adopting the Structural Equation Modelling (SEM) analysis using AMOS, the results indicated that all the fit indices satisfied the recommended range of value. This implies that the model developed was acceptable. The validation results also revealed that the entire model fitness was appropriate and evidence of the stability of the conceptual framework used in this study.

Keywords: Information Flow Performance, SISP, IT Components

1. Introduction

Information flow is the mirror that provides insights into the activities which are carried out in an organization. It also provides a support for the material flow and the activities that directly build up the main products or services of any given organization. In addition, it connects material flow and decision makers of the organization [1]. Therefore, information flow is an important factor taking into enhancing the organizational performance. According to [2], it is often contended that information is now analogous to an organization's lifeblood: should the flow of information become seriously restricted or compromised then the organization may wither and die. This section, therefore,

defines the information flow from different perspectives. It assists us to enhance our understanding of information flow better with a particular emphasis on the security of information flow. According to [3], efficient information flow is a crucial part of any organizations operational processes. Having a well-organized information flow can provide a competitive advantage to a company.

As pointed out by [4], information flow includes information transferring and feedback across organizations. It plays an important role in enhancing the performance of organizations [5-6] argued that efficient information flow implies a need for a security. Therefore, securing efficient information flow is necessary to improve the organizations' performance. According to [7], availability, confidentiality,

integrity and accountability are considered as the main characteristics of security of information flow. They are simplified as access to the right information to the right people on the right time. IT components in Strategic Information Systems Planning (SISP) implementation which include hardware, software, human resources, networking and procedures provide bases to constantly monitor and evaluate the efficiency and effectiveness of the SISP implementation. Moreover, they provide a substantiated evidence to determine progress toward the specific organizational objectives concerning information flow efficiency. According to [8], information flow, the logical design of distributed systems, provides a general theory of regularity that applies to the distributed information inherent in both the natural world of biological and physical systems and the artificial world of computational systems.

A wide number of previous studies have accumulated on different definitions of this concept of information flow and, such concept has been interpreted differently by various authors and researchers in the general field of information theory [9]. In the Lattice Theory of Information, [9] claims that "it is hardly to be expected that a single concept of information would satisfactorily account for the numerous possible applications of this general field". Based on the previous literature in this research area, it is evident that information is a powerful concept which is correlated with several definitions, none of which is being universal. Although all definitions are dependent and related to a specific issue, the concept of information is usually associated with a connotative which is based on two principles. However, based on previous research in information flow, there is a gap in the literature which is the limited empirical evidence on the development and validation of model for improving the Information flow performance. Therefore, this study aimed to develop and to validate a SISP model designed to improve the information flow performance by incorporating the antecedent factors namely; information technology components, information needs and security of information flow factors and it also examined the relationships among these factors.

2. Related Works

2.1. The SISP Approach

The SISP approach is an integration of methods, processes and implementations as well as varieties of activities and behavior upon which organizations have reflected [10]. According to [2], an SISP approach comprises a mixture of techniques, elements, or procedures from different SISP methodologies. As a comprehensive approach, the SISP is not only based on certain techniques, but it involves some formal activities and some informal behavior. The necessary elements in the approach include methods, styles, processes, a focus and a probability of implementation. There are five approaches to the SISP as suggested by [11-12] namely; organizational, administrative, method driven, business led

and technological approach. These approaches have gained credence from an assessment of the extent of the rationality and adaptability of the planning process [13].

The organizational approach assumes that the SISP is based on a continuous integration of organizational and IT functions. The function of IS works in a close partnership with the rest of the organization, especially with managers and executives [11]. This approach emphasizes on management understanding and involvement. Through this approach, the concept of learning organization is important in the development and implementation of the SISP.

The administrative approach concerns the alignment between organizational planning and IT resources of the organization. In this approach, allocation of suitable organizational resources in the planning process is important to ensure the success of SISP. This approach works in tandem with the normal financial planning. The benefit of this approach is that everybody knows about the procedures and all users have the opportunity to submit their proposals.

The method driven approach is about using specific SISP methodologies to ensure the success of SISP adoption. Effective utilization of SISP methodology assists in gaining an opportunity from the SISP process. The technological approach emphasizes the development of SISP process based on suitable/available technology and resources of the organization. Specifically, its emphasis is placed on the assumption that any given IS oriented model of any business is a necessary outcome of the SISP. Therefore, analytical modeling methods are appropriate to be applied in this approach [11].

The last approach is the business led approach. This planning approach highlights the organizational process and activities in the development of the SISP. Affective organizational planning is expected to guide a suitable technological infrastructure to fit in with the organization's needs for information technology. Studies by [11] and [10] indicate that the organizational approach with characteristics such as good alignment, analysis, co-operation, implementation, capabilities, satisfaction and contribution is the best approach in the SISP as compared to the other approach.

[12] empirically analyzed the five SISP approaches and investigated the covariance among these five approaches. The results revealed emerging relations among the approaches. The covariance between administrative and Technological and between organizational and business-led approach is the strongest. The administrative approach has a strong influence on organizational and business-led approach. These findings were supported by the results of the hypotheses tested in the current research.

2.2. Previous Related Review

There are a number of related empirical studies in the scope of information flow, each of which has its own aims and conclusions. The general trend among the discussions of these works is the secure information flow. In addition, the focus was also on improving the organizational information

flow for the purpose of enhancing efficiency and productivity. An empirical study was conducted by [14] aiming at exploring the structure and processes involved in the management of information flow within a closely collaborating value chain systems. The attempt was to establish the nature of information sharing practices employed. In addition, it attempted to identify other key socio-technical factors that could play a vital role in the improved management of information flow.

[15] indicated that the rapid flow of information in the organization strengthens its efficiency. Therefore, a metric was proposed for the speed of useful information as it flows in an organization. Various factors, techniques, and tools can help improve information velocity. According to [15], a direct measure of information flow does not appear to be possible in the near future in light of the given state of technology at the current time. Therefore, a focus on the timing aspect of information flow which deals with time management in organizations is critically needed. [15] described an individual decision-making model that attempts to fill this gap. The researcher proposed formulas for measures and suggests a small, simplified set of questions to obtain a quick metric, and described future research.

In a study by [16] aiming at proposing a methodology to describe the information flow involved in the coordination of production processes, a process was represented as a set of interdependent tasks accomplished by using resources as inputs. Task interdependencies were managed in a way by which resources made decisions and exchange messages according to their decision-making responsibilities. In assessing a process coordination load known as the effort required for resources to address coordination problems, the proposed methodology was found to be valuable for managers in enhancing the adopted coordination form or improving the performed process and supporting the selection of the coordination technologies that better satisfy the information requirements.

An empirical study was also conducted by [17] to develop a model for understanding the importance of combining semantic information and logistics to provide an initial solution to the problem of information overflow. The focus was on how to improve information flow, which is essential and it impacts operational efficiency and organization productivity. The model combines semantic information and logistics as a mean to provide the right person, with semantic information, at the right time and for the right purpose. This combination was a foundation for just-in-time information, also considered as a problem-solving basis for telecom enterprises which could facilitate their daily workload.

According to [18], most of the security of information flow requirements such as the control policies should be considered only after completing the functional requirements. Consequently, less secure systems are developed because security aspects are not properly planned through the early development life cycle. Therefore, there is a need to formally analyze and validate security requirements during the earlier phases of the development to detect and remove design

vulnerabilities before proceeding to other phases [3].

The study by [15] was based on the assumption that information is useful if a member of the organization considers it as a potential to reduce uncertainty, and thus become an important contribution to a decision process. Information velocity depends on information flow and time, which is sometimes described as “getting the right information to the right person at the right time. Efficient information flow is the goal of net-centric warfare and is needed for making faster, efficient, and better decisions.

Effective information flow is critically a key for organization's performance [5]. Information flow takes several forms throughout any given organization on a daily basis. Moreover, information flow also implies information integrity and accuracy. The effective transfer of information is a prerequisite for high-quality decision making and coordinated and organizational action. But, failing to ensure adequate information flow across the organization usually results in issues such as metric information i.e. to receive correct information the right time.

According to [4], information flow includes information transferring and feedback across organizations. The multi-level organizational structure renders many difficulties in information transferring and feedback. In general, multi-layers of the organizational structures play a fundamental role in certifying the ISO 9000 quality assurance systems. Much of the work including quality manuals and procedures document writing, training, internal audit and management review is organized and finished by the quality assurance group in the highest organizational level. Indeed, the plan of quality assurance must be implemented by all operational levels of the organization. Thus, information flow including information transferring and feedback among all the different levels across the organization forms the necessary foundation for effective quality management and quality assurance.

The ISO 9000 quality assurance systems highlight more effective information exchange in quality management. Assumably, the information is transferred from a high level to a low level (that is from decision making level to middle and operational levels), and information feedback is from low to a high level. As indicated earlier, organizations face difficulties in sharing information among participants. In general, two major kinds of information flow include information transferring from operational levels to middle and strategic levels and information exchange between operational units.

3. Method

3.1. Research Hypothesis Formulation

The following research hypotheses were formulated based on the following relationships among several constructs:

(1). The relationship between the availability of the IT basic components and the information needs: The attention here is focused on knowing the needs of the administrative hierarchy for the organization and whether the IT basic

components meet the needs according to the perspectives of the respondents or not which is expressed in the following research null hypothesis.

H01: There is no statistically significant effect for the independent variables IT components on the dependent variables (external and internal information needs).

(2). The relationship between the availability of the IT basic components and the security of information flow in the practical work situation in the institution: This is concerned with the relationship between the IT basic components and the security of information flow (confidentiality, integrity, availability of information flow, accountability) according to the respondents'. It also concerned with whether the SISP provides a security of information flow effectively and efficiently in the institution. To recognize this relationship, the second research null hypothesis was formulated as follow:

H02: There is no statistically significant effect for the independent variables (software, hardware, human resources, networks and procedures) on the dependent variable the security of information flow (confidentiality, integrity, availability of information flow, accountability) according to the respondents' views.

(3). The relationship between the availability of the information needs and the security of information flow in the practical work situation in the institution: In this part, the attention is focused on knowing the needs of the administrative hierarchy for the organization and to study their influence on the security of information flow factors (confidentiality, integrity, availability of information flow, accountability). To recognize this relationship, the following null-hypotheses were formulated:

H03: There is no statistically direct or indirect effect for the independent variables (external and internal information needs) on the dependent variable the security of information flow (confidentiality, integrity, availability of information flow, accountability) according to the respondents' views.

3.2. Data Collection

The current study used a self-administered survey for the data collection. The survey was administered to three hundred and fifty (350) employees at the Ministry of Higher Education and Scientific Research (MoHESR) and four (4) government universities in Yemen. Out of the total number of participants, 62.3% responded to the questionnaire. The major aim of carrying out this survey was to collect data for evaluating the information flow performance in the MoHESR and universities in Yemeni in terms of its benefits or advantages brought up by its application to the MoHESR and these institutions for carrying out the achievement of their goals effectively. Thus, the survey consisted of three dimensions which are IT component, information needs and security of information flow. These three components comprise specific elements. Concerning the IT components, there are five elements; hardware, software, networks, human resource and procedure. For security of information flow, there are four specific elements: confidentiality, integrity,

availability and accountability.

3.3. Data Analysis

Before analyzing the data, both constructs and the items in the constructs needed to be validated. To ensure the validity of the constructs, factor analysis was performed on the variables' items. To ensure the reliability of the items used in measuring the construct, exploratory factor analysis (Stefanek) was conducted using principal components as means of extraction and VARIMAX as the method of rotation. EFA was conducted to check the discriminant and convergent validity. This analysis was performed on the three main components of information flow performance.

The study adopted the "Principal Axis Factoring" as the extraction method and 'VARIMAX' as the rotation method since these two methods have been adopted by most previous researchers [19, 20, 21, 22]. The study also adopts the result cut-off loading point. Eigenvalue, which refers to the amount of variance that a component or factor can account for of eigenvalue of greater than 1.0. In this study, the eigenvalue and total variance explained on all the three factors are as shown in Table 1, Table 2 and Table 3, respectively.

From the extraction results, there are five factors extracted with Eigen value greater than 1 from the first factor (IT components). The first factor is categorized as the human resources factor and the second factor is the procedures factor. The third factor is the networking factor, and the forth factor is the hardware factor.

Table 1. Total Variance and Eigenvalue for IT Component Factors.

Components	Eigenvalues	% of Variance	Cumulative %
Human resources	7.320	29.281	29.281
Procedures	2.627	10.508	39.789
Networking	2.044	8.175	47.964
Hardware	1.624	6.496	54.460
Software	1.255	5.020	59.481

The fifth factor is the software factor. The result of the analysis is indicated that the human resources factor has the largest Eigen value of 7.32 which explains about 29.281% of the variance. In total, the five factors explain about 59.481% of the variance amongst the IT components factors. From the extraction results, we extracted two factors with Eigen value which is greater than the second factor (information need) with 1. It is categorized as the internal information needs factor and the external information factor. The results of the analysis are which indicated that the internal information need factor has the largest Eigen value of 5.08 that explains about 50.82% of the variance.

Table 2. Total Variance and Eigen value for Information Need Factors.

Components	Eigen value	Variance of %	Cumulative %
Internal information need	5.082	50.822	50.822
External information need	1.345	13.451	64.273

From the extraction results, there are four factors extracted with Eigen value 1 greater than from the third factor (security of information flow). The first factor is categorized as the

integrity factor, and the second factor is the accountability factor. The third factor is the confidentiality factor and the fourth factor is the availability of information flow factor. The results of the analysis indicated that the integrity factor has the largest Eigen value of 4.899 that explains about 30.61% of the variance. In total, the four factors explain about 65.80% of the variance amongst the security of information flow factors.

Table 3. Total Variance and Eigen value for the security of information flow.

Components	Eigen values	% of Variance	Cumulative %
Integrity	4.899	30.617	30.617
Accountability	2.913	18.205	48.822
Confidentiality	1.585	9.904	58.726
Availability	1.133	7.080	65.806

3.4. The Structural Equation Modeling Analyses

This section reports how Structural Equation Modeling (SEM) proposed by Semiawan & Middleton (1999) was used to analyze the results for constructing the proposed model. The SEM is considered adequate for the type of investigation carried out by this study since it allows for answering questions that involve multiple regression analysis of factors among a single measured dependent variable and a group of measured independent variable [23]. Thus, the current

research followed five steps of SEM the important is three, using the software AMOS 16 [18] as synthesized from various SEM authors such as [24-30]; Bollen 1989.; Diamantopoulos 1994; Hair 2006.; Hausman 2001.; Kline 1998.; Tabachnick & Fidell 2012).

4. Findings

4.1. Results of the Relationship Between Information Needs and It Components

The purpose of this investigation was to test if there was any significant relationship between IT components and information needs as previously assumed in H01. The measurement and structural model for the above relationship is shown in Fig 1. Direct path was specified from the information needs to IT components which include.

The fitness of the model was examined by using the SEM analysis for the verification purposes. The goodness-of-fit estimating the above relationship model between the information needs and the IT components was examined and the results were represented in Table 4. In this structural model, it was found that all the indices satisfy the recommended values which indicate that the model fitness was excellent.

Table 4. Measures of Model Fitness: information needs and IT components.

FitMeasure	Recommended Value	Fitness Measure	Conclusion
χ^2		54.798	Acceptable
χ^2/df	< 3.0 (Medsker et al.,1994)	2.383	Acceptable
CFI	> 0.90 (Gefen et al.,2000)	0.931	Acceptable
IFI	\geq 0.90 (Benteler & Bonett,1980)	0.933	Acceptable
RSMEA	< 0.09 (Browne & Cudeck,1992)	0.08	Acceptable

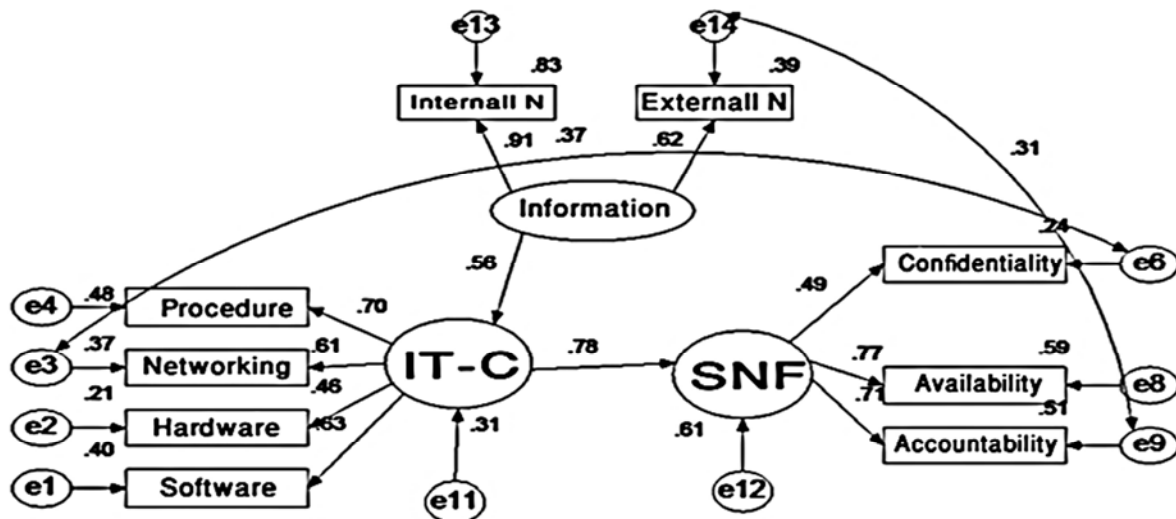


Figure 1. Information Need-IT component-Based Model.

The first path from information needs to IT components was investigated. The standardized coefficients R2 for this path is 0.56, which is significant at p<0.000. In addition, the effect size of information needs in IT components is 0.31. Therefore, the hypotheses H01: there is a significant relationship between information need and SISP in the

MoHESR and universities in Yemen” is strongly supported.

4.2. Results of the Relationship Between It Components and Security of Information Flow

The purpose of this investigation was to test if there was any significant relationship between IT components and

security of information flow as previously stated in H02. The measurement and structural model for the above relationship is shown in Figure 2. Direct path was specified from IT components to security of information flow. The fitness of the model was examined by using the SEM analysis for the verification purposes. Based on this, it was revealed that the

goodness-of-fit estimating the above relationship model between IT components and security of information flow was examined and the results are presented in Table. 5 In this structural model, all the indices were found to satisfy the recommended values which indicate that the model fitness was excellent.

Table 5. Measures of Model Fitness: IT components and security of information.

Fit Measure	Recommended Value	Fitness Measure	Conclusion
χ^2		54.798	Acceptable
χ^2/df	< 3.0 (Medsker et al.,1994)	2.383	Acceptable
CFI	> 0.90 (Gefen et al.,2000)	0.931	Acceptable
IFI	\geq 0.90 (Benteler & Bonett,1980)	0.933	Acceptable
RSMEA	< 0.09 (Browne & Cudeck,1992)	0.08	Acceptable

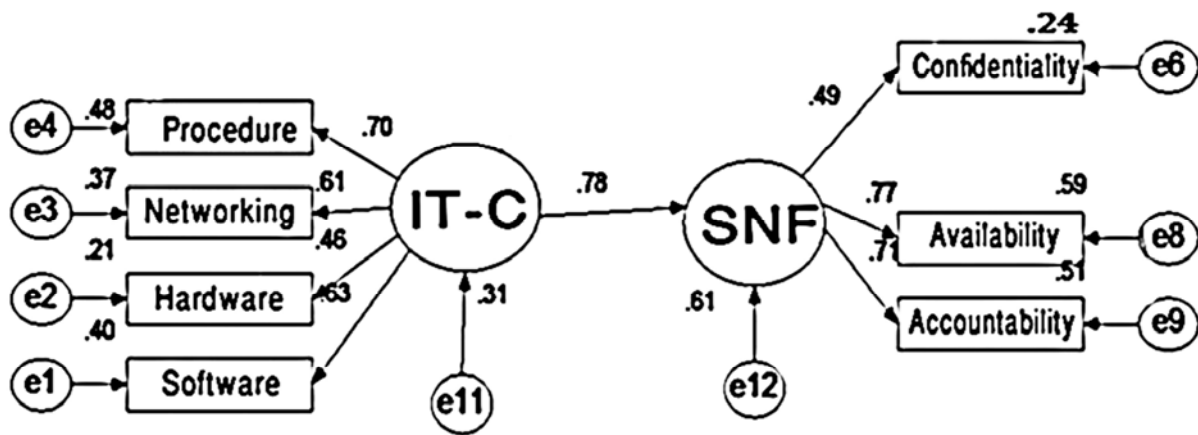


Figure 2. IT components-security of information flow-Based Model.

The second path from IT components and security of information flow was investigated. The standardized coefficients R2 for the path from IT components to security of information flow is 0.78, which is significant at $p < 0.000$. In addition, the effect size of IT components in security of information flow is 0.61. Therefore, the hypothesis 'H02: There is a significant direct relationship between IT components and security of information flow in the MoHESR and universities in Yemen, is strongly supported.

4.3. Investigating the Relationship Between Information Needs and Security of Information Flow

The purpose of this investigation was to test if there was

any significant relationship between information needs and security of information flow as previously mentioned in H03: The measurement and structural model for the above relationship is shown in Figure 3. Indirect path through IT components was specified from information needs to security of information flow. The fitness of the model was examined by using the SEM analysis for the verification purposes. The results revealing that the goodness-of-fit estimating the above relationship model between information needs and security of information flow as examined are presented in Table 6. In this structural model, all the indices were revealed to satisfy the recommended values which pointed out that the model fitness was excellent.

Table 6. Measures of Model Fitness: information needs and security of information flow.

Fit Measure	Recommended Value	Fitness Measure	Conclusion
χ^2		54.798	Acceptable
χ^2/df	< 3.0 (Medsker et al.,1994)	2.383	Acceptable
CFI	> 0.90 (Gefen et al.,2000)	0.931	Acceptable
IFI	\geq 0.90 (Benteler & Bonett,1980)	0.933	Acceptable
RSMEA	< 0.09 (Browne & Cudeck,1992)	0.08	Acceptable

The third path from information need to security of information flow was investigated. The standardized coefficients R2 for the path from information needs through IT components to security of information flow is $0.56 * 0.78 = 0.43$, which is significant at $p < 0.000$. Therefore, the hypothesis 'H03: There is a significant indirect relationship between IT components and security of information flow

through IT components in the MoHESR and universities in Yemen, is moderately supported.

4.4. Investigating and Validating the Proposed Model

Based on the results obtained and analyzed from the data collected through the survey, a comprehensive security of information flow model was developed Fig. 4.

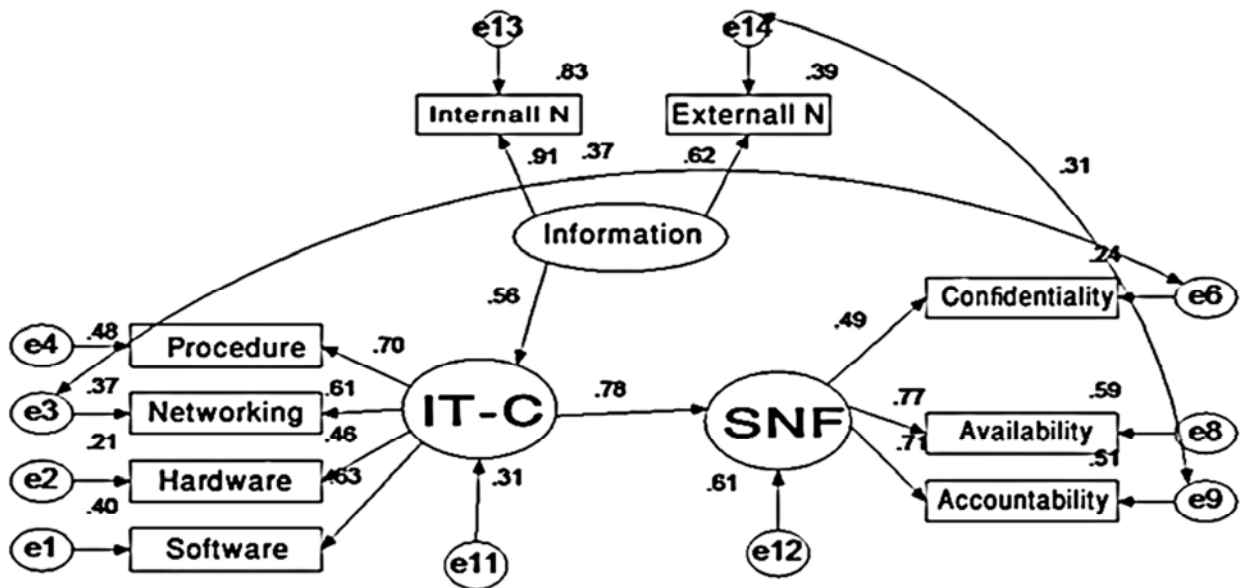


Figure 3. Information need-security of information flow - Based Model.

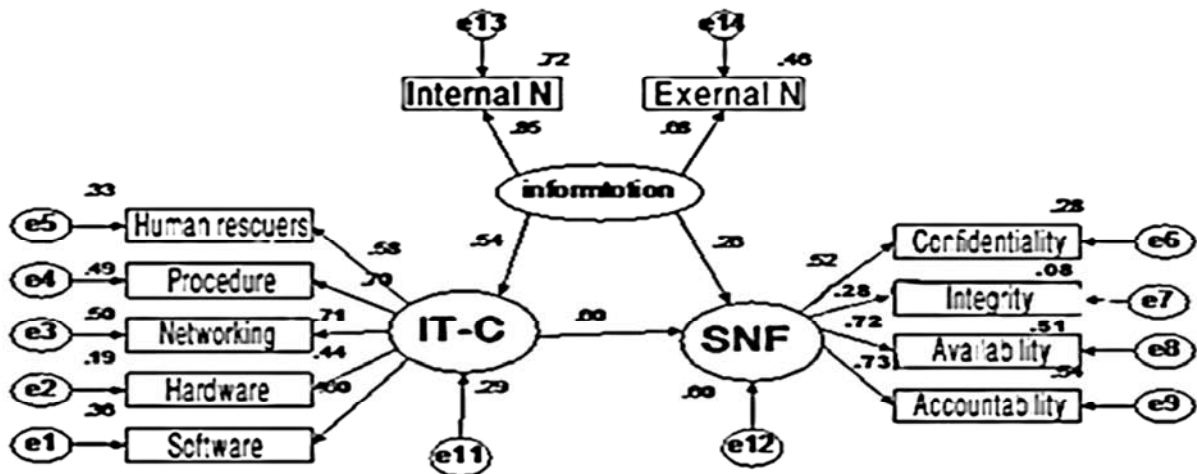


Figure 4. The Comprehensive Developed Model of information flow performance.

The most difficult part of this process was to obtain the fitness of the model with the empirical data or the validation process. Therefore, during the development of the proposed security of information flow model, the following tasks needed to be performed. The first task was constructing the structural model entirely by combining all the models

(previously tested and validated) and integrating the component models into the security of information flow. The second task was validating the developed information flow performance model by measuring the goodness-of-fit as shown in Table 7.

Table 7. Measures of The Comprehensive Developed Model of information flow performance Fitness.

Fit Measure	Recommended Value	Fitness Measure	Conclusion
χ^2		176.672	Acceptable
χ^2/df	< 3.0 (Medsker et al., 1994)	4.309	N. Acceptable
CFI	> 0.90 (Gefen et al., 2000)	0.774	N. Acceptable
IFI	\geq 0.90 (Bentler & Bonett, 1980)	0.779	N. Acceptable
RSMEA	< 0.09 (Browne & Cudeck, 1992)	0.134	N. Acceptable

From the results of the SEM analysis using AMOS 16.0, the measures of fitness of the developed comprehensive model were obtained (as shown in Table 7). As shown in Figure 5 and Table 7, the developed comprehensive information flow performance model did not satisfy the

criteria of goodness-of-fit indices as suggested by previous researchers. Therefore, the developed model was refined through dropping insignificant loading factors and relationships.

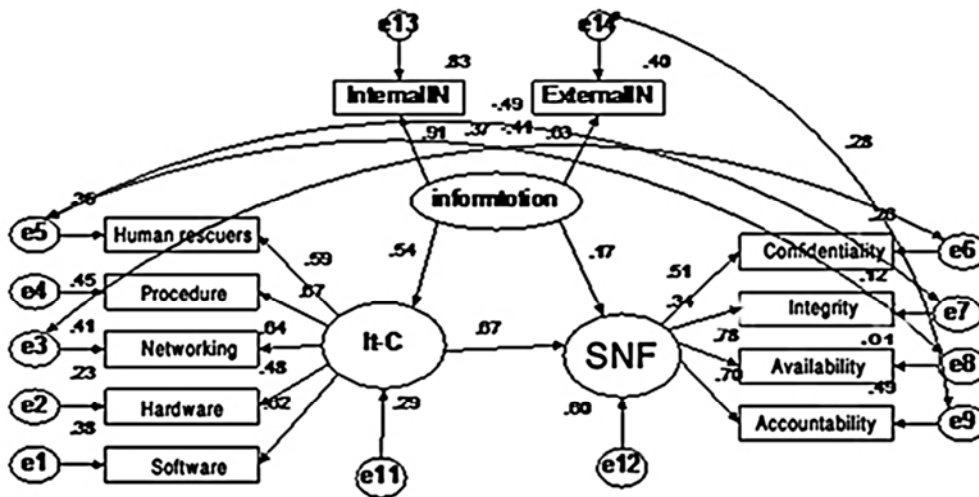


Figure 5. The graphic representation of the developed comprehensive model of the information flow performance Fitness in the Pre-Refining Process.

Looking at the comprehensive developed model, all factor loadings were significant ranging from 0.44 to 0.85 except the integrity loading factor (0.23). In addition, all the relationships were significant ranging from 0.54 to 0.60 except the direct relationship between information need and security of information flow (0.26). Also, a close look at the parameter estimates in Figure (6) showed that human resources factor are correlated with two of the security of information flow loading factors (integrity and availability). Therefore, we dropped these loading factors and the

relationship from the model to refine the model.

After dropping these factors, we estimated the parameters, and the new measures of fitness obtained are shown in Table 8. Based on these results, the new information flow performance model as shown in Figure 5 satisfies the criteria of goodness-of-fitness indices as suggested by previous researchers. Therefore, the model fits the empirical data well. The fitness measures obtained in this research were as the recommended values. (For more details about the model and the model fit, refer AMOS tabular output in Appendix G).

Table 8. Measures of Model Fitness: the modified model.

Fit Measure	Recommended Value	Fitness Measure	Conclusion
χ^2		54.798	Acceptable
χ^2/df	< 3.0 (Medsker et al.,1994)	2.383	Acceptable
CFI	> 0.90 (Gefen et al.,2000)	0.931	Acceptable
IFI	\geq 0.90 (Benteler & Bonett,1980)	0.933	Acceptable
RSMEA	< 0.09 (Browne & Cudeck,1992)	0.08	Acceptable

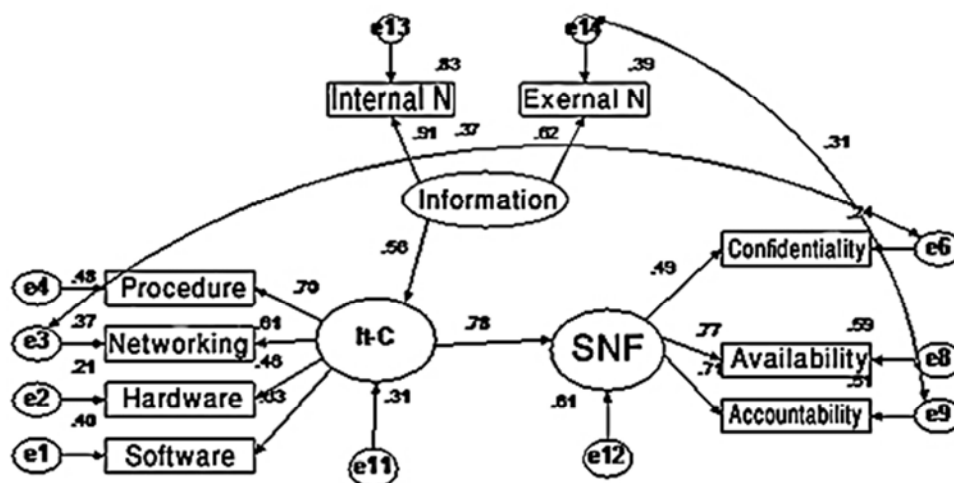


Figure 6. The graphic representation of the modified model of the information flow performance.

Thus, based on the results obtained in the current study, a comprehensive model Fig. 6. was developed. This model includes three kinds of factors namely; independent factor

(IT component), dependent factor (Security of information flow) and mediator factor (information needs). According to the obtained results as represented in this model, the various

relationships among these three factors are explained and discussed. First, the results showed that the IT components have significant influence on the efficiency of security of information flow. The developed comprehensive model indicates that the SISP-IT components provide an effective environment for analyzing, planning, implementing and controlling the efficient security of information flow in the MoHESR and universities in Yemen. The developed model also revealed that understanding information needs of organizational subunits significantly contributes to enhancing the performance of IT components. The effect size of the information needs on the performance of IT components is high. Based on the results previously discussed, the exploratory analysis also revealed that understanding, exploring and assessing the information needs of organizational subunits can significantly contribute to enhancing the organization's information flow. In addition, the results showed that identifying the right information needs, the purpose for which the information is provided and how information is being used are important since they have indirect significant influence on the organization's information flow.

5. Conclusion

The current study aimed at developing a comprehensive model of information flow performance, and the data was collected through administering a survey to five centers of information and technology in the MoHESR and five universities in Yemen. The results of the correlation analysis revealed that there were significant relationships among the investigated factors in the current study. Furthermore, based on the analysis of the results, the study provided evidence of the fitness of the model. The results showed that the fitness of the developed model was acceptable based on the standardized measures suggested by previous researchers.

Acknowledgments

The authors wish to express gratitude to the management of Ibb University Yemen for their support.

References

- [1] Petrauskas, V. 2006. The Use of Information Flow Analysis For Building An Effective Organization. *Information Technology and Control*. 35. (4).
- [2] Doherty, N., Marples, C. & Suhaimi, A. 1999. The relative success of alternative approaches to strategic information systems planning: an empirical analysis. *The Journal of Strategic Information Systems* 8 (3): 263-283.
- [3] Nuseibeh, B. & Easterbrook. S. 2000. Requirements engineering: a roadmap, at: 35-46. O'Brien, R. C. 1995. Employee involvement in performance improvement: A consideration of tacit knowledge, *commitment and trust*. *Employee Relations* 17 (3): 110-120.
- [4] Zeng, S. X., Lou, G. X. & Tam, V. W. Y. 2007. Managing information flows for quality improvement of projects. *Measuring Business Excellence* 11 (3): 30-40.
- [5] Martin, P. 2005. Enhancing effective communication of statistical analysis to non-statistical audiences. *Paper presented at International Association for Statistics Education* 4: 5th.
- [6] Chudnov, A. & Naumann, D. A. 2010. Information flow monitor inlining. *In In Proc. IEEE Computer Security Foundations Symposium: IEEE*.
- [7] Åhlfeldt, R.-M., Spagnoletti, P. & Sindre, G. 2007. Improving the Information Security Model by using TFI New Approaches for Security, *Privacy and Trust in Complex Environments*. In. Venter, H., Eloff, M., Labuschagne, L., Eloff, J. & Von Solms, R. (eds.) 73-84 Springer Boston.
- [8] Barwise, J. & Seligman, J. 1997. Information flow: the logic of distributed systems. Vol. 44: Cambridge Univ Pr.
- [9] Floridi, L. & Sanders, J. W. 2005. Internet ethics: The constructionist values of Homo Poieticus. The impact of the internet on our moral lives.
- [10] Suhaimi, M. A. 1998. An investigation of successful strategic planning of information systems within large companies in the United Kingdom, *Loughborough University*.
- [11] Earl, M. J. 1993. Experiences in strategic information systems planning. *MIS quarterly*: 1-24.
- [12] Pita, Z., Cheong, F. & Corbitt, B. Approaches and Methodologies for Strategic Information Systems Planning: An Empirical Study in Australia, at ChristchurchPita. *Paper read at 19th Australasian Conference on Information Systems Approaches to SISP: An Empirical study in Australia*.
- [13] Liu, H., Yang, H., Yang, J. & Dai, R. 2008. Study On A Model of The Equipment Mro Service Information Systems. *Management Science And Engineering* 2 (2): 43-48.
- [14] Bailey, K. & Francis, M. 2008. Managing information flows for improved value chain performance. *International Journal of Production Economics* 111 (1): 2-12.
- [15] Waters, J. 2009. Information-Velocity Metric for the Flow of Information through an Organization: *Application to Decision Support*: DTIC Document.
- [16] Albino, V., Pontrandolfo, P. & Scozzi, B. 2002. Analysis of information flows to enhance the coordination of production processes. *International Journal of Production Economics* 75(1-2): 7-19.
- [17] Kajtazi, M. 2009. How to improve information flow in telecom enterprises.
- [18] Alghathbar, K. 2009. Enhancement of Use Case Diagram to Capture Authorization Requirements, at: 394-400.
- [19] Koh, C. E., Prybutok, V. R. & Zhang, X. 2008. Measuring e-government readiness. *Information & Management* 45 (8): 540-546.
- [20] Lederer, A. L. & Sethi, V. 1991. Critical dimensions of strategic information systems planning. *Decision Sciences* 22 (1): 104-119.

- [21] Lederer, A. L. & Sethi, V. 1992. Root causes of strategic information systems planning implementation problems. *J. Manage. Inf. Syst.* 9 (1): 25-45.
- [22] Sakri, S. b. 2007. Factors influencing information and communications technology (ICT) abuse in the Malaysian public sector, *Universiti Kebangsaan Malaysia*.
- [23] Ullman, J. 2007. Structural Equation Modelling. In: B. G. Tabachnick and L. S. Fidell, *Using Multivariate Statistics*. US: *Pearson Education Inc.*, 676-780.
- [24] Baumgartner, H. H., C. 1996. Application of structural equation modelling in marketing and consumer research: a review. *International Journal of research marketing* 13: 139-161.
- [25] Bollen, K. A., ed. 1989. *Structural equation with latent variables*. New York *John Wiley & sons*.
- [26] Diamantopoulos, A. 1994. Modelling with LISREL: a guide for the uninitiated. *Journal of Marketing Management* 10: 105-136.
- [27] Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E. & tatham, R. L., ed. 2006. *Multivariate data analysis*. New Jersey: *Pearson International Edition*.
- [28] Hausman, R. 2001. Variations in relationship strength and its impact on performance and satisfaction in business relationship. *journal of Business and Industrial Marketing* 16(7): 600-616.
- [29] Kline, R. B., ed. 1998. *principles and practices of structural equation modelling*. New York: *Guilford PRESS*.
- [30] Tabachnick, B. G. & Fidell, L. S. 2012. *Using Multivariate Statistics: Pearson Education, Limited*.

Biography



Muneer Alsurori Currently Assistant professor in Ibb University, Faculty of Science, Department of Mathematics & Computer Science, received the B.sc and M.sc degree in computer science from Sindh University in Pakistan in 1993 and 1995, and Ph. D. in the field of Strategic Information Systems at University Kebangsaan Malaysia in 2013.



Juhana Salim is full professor, Faculty of Information Science and Technology, University Kebangsaan Malaysia. Her main research interest is in the area of Knowledge Technology Strategic Information System.



Khaled Almasni Currently Assistant professor in National Institute of Administrative Sciences, Department of Statistics, Yemen. Recived the Ph.D at Neelain University Khartoum Sudan in 2013.