Valuing Information Technology (IT) and Operational Risk Management

Anass Bayaga
University of Fort Hare
School of Continuing & General Education
abayaga@ufh.ac.za

Stephen Flowerday
University of Fort Hare
Department of IS
Sflowerday@ufh.ac.za

Liezel Cilliers
University of Fort Hare
Department of IS
lcilliers@ufh.ac.za

Valuing Information Technology (IT) and Operational Risk Management

Abstract. *The focus of this study was to investigate the relationship between: (1) information communication technology (ICT) operational risk management (ORM) and (2) performance of small to medium enterprise (SME). To achieve the focus, the research investigated five specific research objectives that included the principal causes of ICT ORM failure in SME: change management requirements; characteristic(s) of business information, new solutions and finally evaluating models for understanding the value of ICT ORM in SMEs.*

From the review of literature, an electronic survey of closed ended questions was developed for a total of 107 responses. Factor Analysis was used as a data reduction technique. It was used to reduce a large number of related variables to a more manageable number.

All five operational risk variables of the current study had evidence to support the notion that there was a relationship between IT operational risk management (ITRM) and SMEs performance. The empirical evidence presented indicated that a significant proportion of aforementioned variables impacted on the performance of a SME. Therefore, the premise of the model in the current study is that there is a strategic impact in terms of the ICT operation and SME performance. The evidence was supportive of the strategic recognition or development by the respondents towards the wider implications of ICT operation.

Keywords: *SME Performance, Operational Risk Management, Information Communication Technology*

INTRODUCTION

The focal point of this study was to investigate the relationship between: (1) information communication technology (ICT) operational risk management (ORM) and (2) performance of small to medium enterprise (SME).

INFORMATION TECHNOLOGY RISK MANAGEMENT

Recent studies on information technology risk management (ITRM) in large organisations have witnessed ideal benefits. Research suggests that ITRM can be used to understand organisational operations and

change management (Smith & Kruger, 2010). One study suggests that information technology (IT) risk is business risk, which is defined and operationalised as:

> … business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events that can potentially impact the business. It includes both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives as well as uncertainty in the pursuit of opportunities (ITGI –2009: 11).

ITGI (2009) operational risk management (ORM) has adopted the following explanationI: It is a relatively new (less than a decade old) management discipline that calls for corporations to identify all the risks they face, to decide which risks to manage actively, and then to make that plan of action available to all stakeholders (not simply shareholders) as part of their annual reports. However, risk management is a process which provides assurance that (a) objectives are more likely to be achieved, (b) damaging things will not happen, and (c) beneficial things will be or are more likely to be achieved.

In contrast, the success of ITRM models and theories in large organisations has shifted focus towards the small business enterprises (SMEs) (Basel Committee on Banking Supervision, 2004).

"However, despite these theoretical explanations there is still a shortage of reliable quantitative models that can provide enough information to analyze IT security investments," particularly in SMEs (Smith and Kruger, 2010: 1). One of the reasons attributable to the shift in paradigm, as suggested by researchers and practitioners of ITRM, is that it serves as a new venue of improved services and potential benefits for SMEs (Gerber and Von Solms, 2005).

Additionally, the study of Standing et al., (2007) identified no main effects "…using project outcome (success and failure) as the repeated measure and job responsibility (IT support, line and executive managers) as the independent factor…" [Ibid: 1156]. However, a significant interaction effect for outcome by responsibility, $F(2, 102) = 4.45$, $p < .05$ was determined. When a *post hoc* analysis (Tukeys HSD and single degree of freedom *F* ANOVA) was conducted, it revealed that "… IT support workers attributed themselves significantly more to IT project success (mean = 0.34) than to IT project failure (mean = 0.33), $F(1, 28) = 5.10$, $p < .05$)" [Ibid: 1156]. The reverse was true for executive managers who took more responsibility for their project failure than their project successes ($p = 0.08$). [Ibid: 1156].Yet, a number of studies have suggested that small businesses have not shown a great interest in ITRM, particularly operational risk management (ORM) (Lam, 2006).

Review of several literatures indicates that ORM, a variation of ITRM, provides a structural form of activities and has become a popular vehicle for risk management of information in industries such as financial and manufacturing (ITGI, 2007). In addition to the aforementioned studies, Standing et al. (2007) highlighted that as a rising management discipline, interest and current development of institutional risk management (IRM) varies across industries and institutions. This suggests that ORM is a tool that can be used to evaluate models for understanding the value of IT and for streamlining a company's operations. In support of this view, another study acknowledged that operational procedures and responsibilities are required to ensure the correct and secure operation of information processing facilities (King III Report, 2009).

Operational risk management emerged in the late 1960s when manufacturing companies started looking for ways to alleviate delivery delays that resulted from large volumes of products and services. The use of ORM however, became popular in late the 1980s and early years (Sholes, 2007). Currently, many large organisations in the United States of America, Canada, and Europe use ORM to support their IT financial and trading activities. The adoption of ORM has also progressed rapidly in Australia (Lam, 2006).

There is an indication that the growing use of ORM has drawn the attention of several academic literatures. A number of success stories published in recent years have claimed to have accrued a variety

of benefits due to ORM adoption, while several studies also confirmed the attainment of some ORM benefits to a varying extent (Calder, 2006).
Nonetheless, in the past, considerable research on ORM was conducted for large business; whereas studies on small and medium enterprises (SMEs) towards the adoption of ORM is a recent phenomenon (ITGI, 2009). Additionally, the majority of these studies are confined to the USA, Canada and Europe. Comparatively less has been researched in Africa and the numbers of studies on ORM adoption in South Africa (SA) remain marginal. Regrettably, a limited number of empirical studies on ORM adoption in SMEs have been undertaken in the Eastern Cape, South Africa (SA). Recently, some conducted studies reflected the use of information technology (IT) among SMEs, but even these studies' objectives delineated from the adoption of ORM in Eastern Cape SMEs (King III Report, 2009).

It is important to note that the study adopted a common industry definition of operational risk, namely "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel Committee on Banking Supervision, 2004: 2). Noting that several categorisations of IT risk have been proposed, for the purpose of this study, the researcher adopts and adapts that of IT Governance Institute (ibid). IT risk has been categorized as the solution delivery/benefit realisation risk, associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes (ITGI, 2009: 11).

ICT EFFICIENCY WITHIN SME'S

There are few suggestions made by literature that show the need for ICT operational risk in SMEs (Information Technology Governance Institute -ITGI, 2003). A few empirical studies show the association between ICT operational risk in SMEs and performance in SME (ITGI, 2003). Those studies found that good ICT operational risk in SMEs can generally improve performance. However, there are others which empirically suggest the existence of indirect relationships between ICT operational risk management in SMEs and performance (Anderson & Choobineh, 2008).

It has been argued that for competition and merger analysis of SMEs, it is important to know the effects of market concentration and past merger on an institution's efficiency (National Credit Regulator, 2008). Additionally, National Credit Regulator (2008) found that ICT operational risk activities contribute significantly to enhancing the efficiency of SMEs. Here they argue that ICT operational in SMEs are activities that may be used to improve efficiency. National Credit Regulator (2008) found that efficiency has positive effects on ICT operational risk in SMEs and interest rate risk capitalization, but a mixed result on the effect of ICT operational risk in SMEs. Then, Standing, Guilfoyle, Lin and Love (2007) show that profit efficiency is sensitive to ICT operational risk in SMEs and insolvency risk, but not to liquidity risk or to a mix of loan products in SMEs. Hence it is expected that by managing these risks, the institution's efficiency is expected to improve. From the literature, it is expected that ICT operational risk in SMEs' practices are associated with the level of efficiency and performance of SMEs.

Related Research: ICT Trends in South Africa

Although ICT operational risk in SMEs is one the key function of financial institutions, very little has been done to date to link ICT operational risk in SMEs with performance (Basel II, 2004). However, conceptually, many discussions are made on the objectives of ICT operational risk in SMEs that provide relationships between ICT operational and SME performance (Basel II, 2004). They state that while directors see ICT operational risk in SMEs as critical, there is real concern ICT operational risk in SME's practices is less focused, which may detract from improving business performance. On other aspects,

Liebenberg and Hoyt (2003) researched a sample of [i]firms that signalled their use of ICT operational risk in SMEs by appointing a Chief Information Officer (CIO) and found that firms with greater financial leverage are more likely to appoint a CIO.

The findings are consistent with the hypothesis that firms appoint CIOs in order to reduce information asymmetry with regard to the firm's current and expected risk profile, noting that this is particularly true for large firms. Liebenberg and Hoyt (2003) provide further evidence that financial institutional investment in ICT operational risk in SMEs during the 1990s helped reduce earnings and loss volatility during the 2001 recession.

A recent study by Sholes (2007) used a hazard model to examine the factors that influence the SME level of ICT. They found that firms who are more levered have more volatile earnings but poorer stock performance are more likely to initiate an ICT program (Sholes, 2007). According to the author, firms that face greater risk of financial distress may benefit from ICT when ICT reduces the chance of costly outcomes (Sholes, 2007). Also it was revealed that firms who are at greater risk of financial distress, that is those with more leverage and less financial slack, are more likely to adopt ICT (Layton, 2007). In addition, there are many studies looking at profitability and its various determinants including operational risk factors (Layton, 2007).A number of empirical studies show that ICT operational risk in SMEs is part of the determinants of profitability (Yeo, 2002; Curley, 2004; King III Report, 2009; ITGI, 2009). Hence, it is expected that by managing these risks well, institutions related to SME profitability are expected to increase. As the survival and success of SME depend on the efficiency with which they can manage risks, ICT operational risk in SME is one of the critical factors in providing better returns to shareholders.

Consistently, it is important to note that this categorization "focuses on the causes of operational risk which is appropriate for both risk management and, ultimately measurement" (ibid: 2). Consequently, this study sets out further details on the effects of operational risk related IT risk.

Specific research questions

Building on prior research related to: (1) impact of information communication technology (ICT) and (2) operational risk management (ORM) in the context of SMEs, the focus of this study was to investigate the relationship between: (1) ICT operational risk management (ORM) and (2) performances of SMEs. To achieve the focus, the research investigated five specific research objectives described below:

- Analysing the principal causes of ICT ORM failure in an SME.
- Assessing the change management requirements for building successful ICT systems in SME.
- Identifying which characteristic(s) of business information play a major role in supporting an organisation's business operations.
- Identifying the challenges posed by ICT ORM new solutions and finally.
- Evaluating models for understanding the value of ICT ORM in SME.

RESEARCH DESIGN

Due to the research objective this research adopted a positivist paradigm which enabled the researcher to adopt a survey design for the unit of analysis, using a case study as the site. The research paradigm refers to the philosophy of the research process (Pallant, 2005). This includes the assumption and values that serve as a rationale for research and the criteria the researcher uses for interpreting data and reaching conclusions (ibid).Thus, a crucial premise of positivism is that there are certain regularities in nature which can be observed and/or discovered. These regularities are called 'laws'. Laws are universal. Another crucial concept is 'causality'; people communicate the way they do because some prior condition

caused them to respond to a message in certain ways.

The study was conducted in two phases; one phase followed a case study design, the other, a survey using a questionnaire. The 'case' in this study was a financial company in the Eastern Cape. All units within this case form part of the case (managers, implementers, directors, etc). Building on prior research related to the impact of information technology (IT) and operational risk management (ORM) in the context of SMEs, the current research proposes that there is a relationship between IT operational risk management and performances of SMEs. The motive for using a case study was to understand the complexity such as an organisation. It extends experience or adds strength to what is already known through previous research.

Instrumentation

The items were adapted and administered online electronically after the focus and contestations from literature. First, the research instrument sought information about basic demographics (Fidell, 2009). In order to address the focus, one of the parts addressed the principal causes of ORM failure in SME; it also addressed the change management requirements for building successful systems-risk monitoring and reporting of ORM in SME (ibid). Next were characteristic(s) of business information and this was followed by the challenges posed by ORM new solutions and evaluating models for understanding the value of ICT in SME. This was done by identifying the traditional and modern capital budgeting models and how their drivers impact on business processes.

From the review of literature, an instrument (closed ended questionnaire) was developed with the aim of covering the research focus. In terms of sample size calculation, Ibid recommend a formula for calculating sample size requirements, taking into account the number of independent variables that a researcher wishes to use; $N \geq 50 + 8m$(m= number of independent variables). Due to the objectives posed, questionnaires were sent to a minimum of N=90 respondents of the SME according to a simple random sampling plan, noting that a total of 107 responses was finally received.

Data analysis technique

Factor Analysis was used as the data reduction technique (ibid). For this reason it was used to reduce a large number of related variables (cf. Table 1: KMO and Bartlett's Test & Table 2: Factor loadings after rotation: Component Matrix) to a more manageable number, prior to using them in other analyses such as multiple regression or multivariate analysis of variance (MANOVA) (ibid).

One of the objectives of this study was to find the factors predicting ICT operational risk within SMEs. Multi- item constructs were used to capture information about different of variables to adopt ICT operational risk. A multi-items construct of the instrument were used. A construct was used to measure five main support items. The items were adapted after literature and research questions.

The study was based upon a survey design to collect the primary data from 107 respondents using a simple random sampling technique.

The questions that guided this technique included: 'What is the underlying factor structure of ORM ICT measures that influence SME as proposed by the current study's instrument?' The items of ORM ICT measuring the influence of SME were subjected to Factor Analysis (FA) - principal component analysis. Five components were eventually retained in the analysis. The items that cluster on the same components suggest that component 1 represents X, component 2 Y, component 3 Z, component 4 K and component 5 L.

Data reduction technique: factor analysis

Factor Analysis (FA) as a technique was designed not to test hypothesis(es) or tell whether a measure is significantly different from another. Instead it was added as a data reduction technique. Thus, it was used to reduce large numbers of related variables to a more manageable number, prior to using them in analyses such as in multiple regression or multivariate analysis of variance (MANOVA) (Pallant, 2005: 172). Consequently, FA sought to answer the question 'what is the underlying factor structure of ORM ICT measures that influence SME as proposed by the current study's instrument?', the items of ORM ICT measuring the influence of SME were subjected to FA - principal component analysis (PCA) - using SPSS version 18.

Prior to performing PCA, the suitability of data for FA was assessed. Inspection of the correction matrix revealed the presence of many coefficients of .3 and above. The Kaiser-Meyer value was acceptable (cf. Table 1), exceeding the recommended value of .6 (Pallant, 2005) and the Barlett's test of sphericity [16] reached statistical significance, supporting the factorability of the correlation of the matrix.

A PCA was conducted on 24 items with orthogonal rotation (varimax). The Kaiser-Meyer-Olkin (KMO) measure as aforementioned verified the sampling adequacy for the analysis, KMO =.61 (Fidell, 2009), and all KMO values for individual items were > .70, which is well above the acceptable limit .5 (ibid) (cf. Table 1: KMO and Bartlett's Test). As mentioned, Barlett's test of sphericity X^2 (276) = 783.39, p = .000, indicated that correlations between items were significantly large for PCA, which was satisfactory (cf. Table 1: KMO and Bartlett's Test).

Table 1: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.61
Bartlett's Test of Sphericity	Approx. Chi-Square	783.39
	df	276.00
	Sig.	.00

An initial analysis was run to obtain eigenvalues of each component in the data. Five components had eigenvalues over Kaiser's criterion of 1 and in combination explained 65.97% of the variance. The scree plot showed inflexions that would justify retaining the five components. Given the large sample size, and the convergence of the scree plot on five components, this was the number of components retained in the final analysis (ibid). Table 1 shows the factor loadings after rotation. The items that cluster on the same components suggest that component 1 represents X, component 2 Y, component 3 Z, component 4 K and component 5 L (cf. Table 2: Factor loadings after rotation: Component Matrix).

Table 2: Factor loadings after rotation: Component Matrix

	Component				
	1	2	3	4	5
Q7	.72				
Q8	.71				
Q9	.70				
Q10	.66				
Q11	.58				
Q12		.58			
Q13		.51			
Q14		.50			
Q15		.43			

Q16	.64		
Q17	-.52		
Q18	.33		
Q19	30		
Q20	.33		
Q21		.45	
Q22		-.40	
Q23		-53	
Q24		.40	
Q25			.46
Q26			.43
Q27			.40
Q28			.60
Q29			.51
Q30			.33

Extraction Method: Principal Component Analysis

Ensuring reliability and validity

The correlation provided directional support for predicted relationships and showed that collinearity among the independent variables was sufficient. The researcher ensured that the validity and reliability aspects of the instrument were carefully developed. The face and construct validity were ensured by developing from a thorough analysis of the literature. Collegial validity was ensured by giving the instrument to specialists in the field of IT risk management to check whether the constructs were represented correctly.

ANALYSIS AND DISCUSSION OF FINDINGS

The current section addresses factor analysis - data reduction, determining the factors for principal causes of ORM failure related to ICT, organisational factors related to change management requirements and ICT risk, characteristic(s) of information influence on ICT risk, challenges posed by ORM solutions, evaluation models affecting ICT adoption within SMEs and ICT operational risk and SMEs performance.

About 107 questionnaires received were analysed using SPSS version 18. The data showed that about 60.7 percent of the respondents were IT personnel, about 23.4 percent finance and 10.3 percent operations staff. The study identified various factors of ICT operational risk in SMEs adoption within the case organisation. Under principal causes of IT failure, the current study revealed that [ii]A was significant in determining the ICT operational risk in SMEs adoption. In other factors studied, A was the only significant ICT operational risk that affected SMEs. Thus, SMEs need to adopt A for ICT operational SMEs, since they would be provided with benefits that could be accomplished through ICT operation.

Although the principal causes of ORM failure related to ICT are important, so too are (1) change management requirements: (2) challenges posed by ORM solutions: and (3) evaluation models. Further emphasis on the relative importance of variables over others showed that [iii]A does have a significant impact on change management requirements. This further indicates that management of the SMEs must focus on A for ICT operational risk benefits compared with the other factors, to gear up the adoption process. Additionally, around half of the percentages of ICT operational risk in SMEs adoption variance were explained. Based upon the results, the current study proposes that in order to obtain the full benefits from ICT operational risk, SMEs must adopt a pro-active approach and focus more on the potential

benefits as aforementioned. Building on prior research in ICT operational risk in SMEs and performances of financial institutions, this current study suggests there are relationships between ICT operational risk in SMEs and performances of SMEs. Specifically, a model developed shows the relationship between ICT operational and performance of SMEs practices. ICT operational risk in SMEs in financial institutions is not a new phenomenon (Anderson and Choobineh, 2008). Dealing with risk has always been the raison d'être of institutions. For instance, financial institutions (SMEs) are in the risk business (National Credit Regulator, 2008). Calder (2006) argues that an integrated, holistic approach to ICT operational risk in SMEs can create shareholder value. Therefore, the effective management of ICT risk in SMEs is crucial to any financial institution's performance. In support of this, Standing et al. (2007) describe ICT operational risk activities designed to minimise negative possible losses. ibid reveal that the purpose of ICT operation is to maximise revenues and offer the most value to shareholders by offering a variety of financial services, and especially by administering risks. Accordingly, ICT operation is central to SMEs.

The survival and success of financial organisations depend on the efficiency in with which they can manage risks; hence, ICT operational risk in SMEs is one of the critical factors in providing better returns to the shareholders (ibid). Also, it will depend to a large extent on how these institutions manage different risks arising from their operations (ibid). This suggests that an effective and efficient ICT operational risk in SMEs financial institutions should assume particular importance as they endeavour to cope with the challenges of globalisation. The findings and for that matter objectives of this current study are thus consistent with previous studies (King III Report, 2009). The next section addresses individual factors of the five main objectives.

IT Operational risk and SMEs performance

Both the current findings and reviewed literature show that performance of SMEs holds significant importance to the variables studied. In fact, a previous study by Basel Committee on Banking Supervision (2004) examined the relationship between ICT and performance of financial institutions (SMEs) and found a mixed result on the relationship between for instance, capital structure and profitability.

From the current study's results, there are particular sub variables of the five main categories that impact on performance of SMEs. However as suggested by literature (Lam, 2006), the major reason noted for not establishing such ICT was the non-IT literacy of customers or the prohibitive costs quoted by consultants for setting up an ICT site. Although the study had identified a slower uptake of ICT usage within HR personnel, it was evident from responses that ICT development was a significant feature in the thinking of most operations in terms of future innovations, a result that perhaps indicates that such development for SMEs is still viewed as an innovative product yet to be fully exploited.

The current study, and comparative studies conducted by Gerber and Von Solms (2005), largely supports suggestions to adopt ICT operations within SMEs business strategies. The belief that ICT provides a potential transformational impact or a solution to key business issues and challenges gives some explanation for the overall level of strategic commitment by respondents.

CONCLUSION

The findings support other similar studies and increase the generalisability of previous researches. At the outset, the ICT adoption was measured on a four-point Likert scale. All five operational risk variables of SMEs of the current study provided evidence to support the notion that there was a relationship between IT operational risk management (ITRM) and SME performance. The empirical evidence presented indicated that a significant proportion of aforementioned variables impacted on the performance of SMEs. Therefore, the premise of the model in the current study is that there is strategic impact in terms of the ICT operation and SME performance. The evidence was supportive of the strategic recognition or development by the respondents towards the wider implications of ICT operation.

RECOMMENDATION

For Methodological Use further research is needed adopting the methodology used in this study that is, factor analysis, and to monitor these changes more closely and to measure the changing strategies and the associated factors such as insufficient or improper user participation in the systems development process, identified as potential barriers to the effective adoption and implementation of ICT strategies. The methodology used in this study, that is factor analysis, can also be applied in different sectors of SMEs, either to study similar factors or emerging factors other than the current study's variables.

REFERENCE

[1] Allen, J. (2005). Governing for Enterprise Security. www.sei.cmu.edu/publications/documents/05.reports. from Retrieved Feb 13, 2010.

[2] Anderson, E.E. and Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security*, 23(3), pp56-69.

[3] Basel II. (2004). The new Basel capital accord. Switzerland: Bank for International Settlements.

[4] Calder, A. (2006). Information Security Based on ISO 27001/ISO 17799. Amersfoort - NL: Van Haren Publishing.

[5] Curley, M. (2004). Managing Information Technology for Business Value. NY. Intel Press.

[6] Fidell, A. (2009). Discovering Statistics with SPSS, London. Sage.

[7] Gerber, M. and Von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, 24 (1), 16-30.

[8] Information Technology Governance InstituteITGI – (2003). IT Governance Institute ITGI-Board Briefing on IT Governance. ITGI Institute. ITGI Press

[9] Information Technology Governance Institute– (2007). IT Governance Institute ITGI"- CobiT 4.1, Executive Summary. ITGI Institute. ITGI Press

[10] Information Technology Governance Institute–(2009). IT Governance Institute, "Enterprise Risk: Identify, Govern and Manage IT Risk. The Risk. ITGI Institute. ITGI Press

[11] King III Report. (2009). King Committee on Governance: code of Governance Principles for South Africa. Pretoria. Pretoria Press.

[12] Lam, J. (2006). Emerging Best Practices in Developing Key Risk Indicators and ERM Reporting, Japan: James Lam and Associates.

[13] Layton, T. (2007). Information Security: Design, Implementation, Measurement and Compliance. Boca Raton: Auerbach Publications.

[14] Liebenberg, A. and Hoyt, R. (2003). The determinants of enterprise risk management: evidence from the appointment of chief risk officers. *Risk Management and Insurance Review.* 6 (1), pp. 37–52.

[15] National Credit Regulator, (2008). About the NCR. from rhttp://www.ncr.org.za/the_NCR.html, Retrieved February 21, 2009.

[16] Pallant, J. (2005). SPSS; Survival Manual. London: Open University.

[17] Sholes, M. (2007). Risking Business Value from www.mhmonline.com/view. Retrieved February 3, 2009

[18] Smith, E.H. and Kruger, H.A. (2010). A framework for evaluating IT security investments in a banking environment." Information Systems South Africa (ISSA) 2010 Conference: ISSA 2010, Proceedings published by the IEEE Online. Retrieved Jun 9, 2010

[19] Standing. C., Guilfoyle A., Lin, C. and Love, P.E.D. (2007). The attribution of success and failure in IT projects, Industrial Management & Data Systems, 106, pp 1148-1165.

[20] Yeo, K.T. (2002). Critical failure factors in information system projects. International Journal of Project Management, 20 (3), pp 241-246.

[i] In this study the words firms, organisation, institution and business are used interchangeably.

[ii] One of the principal causes of information system failure is insufficient or improper user participation in the systems development process.

[iii]There is a high failure rate among enterprise application projects because they require extensive organizational change that is often resisted by members of the organization.