European Journal of Business and Management
ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online)
Vol.8, No.29, 2016

Efficiency of Accounting Information System and Information Security Investment Impact on Firms Performance: A Review

Susan Peter Teru[1*] Daw Hla[2] Innocent Idoko[3] Al-Mustafa Tafida[3]
1. Faculty of Social Sciences, Taraba State University Jalingo, Nigeria
2. Faculty of Economics and Business, Department of Accounting and Finance, Universiti Malaysia Sarawak
3. Faculty of Social Sciences, Taraba State University, Nigeria

Abstract
Accounting Information systems should be kept safe and protected at any moment because it contains a very sensitive and confidential information. It has become vital for firms to secure their information securely as a threat to information is rapidly increasing in malicious attacks on the firms' IT infrastructure in which it could affect business continuity. Also, penalties of inadequate security could make firms suffer substantial fiscal loss. As information technology is playing a major role in our businesses and organization today, the rate of security threats also increases, firms are encouraged to invest in a comprehensive and strong IT security set- ups to protect and safeguard the accessibility, integrity, confidentiality of accounting information from vulnerable of threat because it can cause substantial financial consequences, losing of customers, and impairment of good will amongst others. Thus, the drive of this research is to evaluate the impact of firm's investment on information security and accounting information system efficiency on the performance of firms which indicated that a good internal control ensures reliable financial report for decision making, in which the qualitative method of data collection was used which the previous literature was reviewed and other secondary data was also used for the purpose of the study. From our findings, we discovered that unceasing investments on information security procedures lessens the risk of attack from cyber threats and failure of information system. The researchers therefore commend businesses and organizations to take a vigorous method to information security plans and control. Also, to regulate the IT menace of some security occurrences, it is essential for firms to progressively invest in diverse security technologies considering the significant information technology related and non-information technology related security investment factors, and it is vital for businesses and organizations to know the impact of information security investment on performance.
Keywords: Accounting Information System, Firm performance, Investment, Security Technology.
Abbreviation
AIS - Accounting Information System
IT - Information Technology.

INTRODUCTION

Advancement in the technology world has precise to a novel systems of accounting, new models in economics, and businesses transacted on the internet. The advances have lessened the period and rate of the businesses by simplifying improved dealings. Several organizations primarily use the information system to advance proficiency of business events by systematizing present processes. Nowadays, firms and businesses are changing faster with globalization technology, the accounting information system is one and part of this changes and development, this change is contingent on the data and information it produces for the internal and external users for decision making, and reliable financial reporting. Businesses ought to gather reputable data that will produce a valuable information about the business that can help in guiding the users in making the right decision.

The fundamental role of accounting information system (AIS) is to gather data and processes this data to information that can sparingly influence upon firms. AIS processes information and transmit this valuable information to the users. Businesses and managers cannot disregard information systems for they perform a solemn part in the present-day business dealings, Laudon and Laudon, (1991). An efficient AIS can also help in refining the business dealings and effective decision making by the users by providing substantial information at the accurate time. Efficient AIS also helps in sharing knowledge and proficiency, thus improving operations Romney and Steinbart (2003).

Investment in firm's information security has become constantly important to organizations and businesses. Gordon, Loeb, and Lucyshyn (2005) affirms that internet based businesses and organizations can be distressed by security threats and computer incident which can be a serious issue that can affect their business operations. The incidences may include rejection of service, internet scam, illegal admittance to information, virus, monetary scam, net access insider abuse, etc. Whenever accounting information is altered or erased, it generates mayhem calling into queries of trustworthiness or accurateness of the data. Carr, (2003) opined that, in this technology society, businesses and organizations are encouraged to manage several threat in information technology mechanisms rather than using it for competitive benefits.

Therefore, this study paper presents a reflection, based on a literature review which the data was obtained

and examined by making reference to the existing literature so as to compare and contrast different views offered by different authors on the impact of security investment and efficiency of accounting information system on firms' performance. The study tries to look at the factors that makes the accounting information system efficient and the importance of investing in the firms' information security.

REVIEW OF LITERATURE

Information security investment is an allocation of resources to improve or protect the information security of the organization, the products, and services. According to Loch, Carr and Warkentin, (1992), the modern business dealings is profoundly reliant on information via computer systems. It is substantial for organizations to invest in a comprehensive and robust IT security set-up to guard their information systems from several risk of cyber threat.

Karanja and Zaveri (2014) affirms that organization nowadays experience serious security threat due to the speedy increase in both capacity and frequency of nasty attacks on their infrastructures. Hence, they assumed that to protect and ensure confidentiality, integrity and availability of their information, firms should ensure and make sure all the required security guards are in place.

The application of resourceful AIS is an expensive process, which needs substantial exertion, period and resources at all stages of the systems life cycle. So many researchers revealed that the fit between accounting and contextual factors, or between IT and contextual factors, have significant impact on performance (Bharadwaj, Bharadwaj, and Konsynski, 1999; Melinda and Stephen, 2001; Holden and El-Bannany, 2004; Ismail and King, 2005. Such investment pays to the organization's successive long-term efficiency and productivity. An effective project administration in systems operations, and good training and skills development for the systems users are key features in accomplishing efficient AIS Wynn and Maldonado, (2007). It is also reliant on the knowledge of how to use these systems in an effective way that will back the needs of the decision makers and strategic planners in which it can entail change and developments in the basic processes of business of the organizations.

Information systems must be allied with the organization to communicate useful information that the users require within the organization. The organization also must be conscious of, and be logical to the impacts of information systems to be able to benefit from new technology. One key area of the impact in the introduction of information systems is in the development or redesign of main business processes Laudon and Laudon (2005).

Beynon-Davies (2002), affirms that the impact of an information system can be measured in so many ways; on individual bases, on groups, and on the entire organization in which the effects may be negative or positive. Hence, the acceptance of an information system in an organization may cause both planned and unplanned impact. Shaheen, (2012) took a research on a topic factors that affects the effectiveness and efficiency of accounting information systems in Palestinian commercial banks in which his outcome displays that there is a relationship between AIS and environment, technological, legal and cultural factors. Thus, he concluded that the impact of these variables differs, sometimes contingent on the level of administration and backing. There are also several researchers who had discovered aspects that affect accounting information systems efficiency, for example, (Qatawneh, (2005), Hakim (2007), Haddad and Atmeh (2009), Ramly, 2011).

THE EFFICIENCY OF ACCOUNTING INFORMATION SYSTEM.

The most important ingredient in any accounting information system is sound internal control system. AIS can be sustained if there is a sound internal control system Topash, (2014). Masli, Peters, Richard, (2010) defined internal control as a process, affected by the management, an entity's board of directors, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives like reliability of financial reporting, compliance with applicable laws and regulations and effectiveness and efficiency of operations. Effective internal control systems are essential for successful operation of business as well as accounting control and administrative control. It helps the Accounting Information Systems division to generate reliable and relevant information. In the AIS environment the qualities of internal controls adaptation affect operations and management and in the turn influence internal control. Internal controls are run to ensure the achievement of operational goals and performance.

Toposh (2014), Internal controls are measures set up to protect assets, ensuring accounting reports are reliable, encourage efficiency and compliance to company policies. Internal controls are vital to realizing some aims of an organization like efficient and logical manner of accounting communications, safeguarding the assets in adherence to management policy, prevention of error and detection of error, prevention of fraud and detection of fraud and guaranteeing accuracy, completeness, reliability and timely preparation of accounting data. If good internal control ensues in any organization, management can use information with better reliance to continue their business events suitably which provide efficient AIS, but where an organization does not have a sound internal control, management cannot achieve its desired goals. He also alleged that the following measures or indicators are meant to be present in any accounting information system for it to be efficient in any organization; cost effectiveness, good documentation, existence of proper security measures, independent internal and external audit, separation of other operation from accounting, and effective internal control.

Marshal and Romney (2015) affirms that accountants and systems developers can aid management in

attaining their control aims by,

- Designing effective control systems that take a positive method to monitoring systems to detect, correct, and recover from threats when they arise.
- Making it easier to build controls into systems at the early design phase than to add them after the facts
- Businesses or organizations need a detailed understanding of information technology abilities and risk as well as how to use IT to accomplish some organizational control objectives.

ACCOUNTING INFORMATION SYSTEM AND CYBERSECURITY

In examining the modern business environment, the internet is a serious infrastructure used by many organizations in which it is becoming necessary for internet based businesses and organizations to invest more in information security because accounting systems contains sensitive and confidential information that need to be protected and kept safe at any point in time. Whenever organizations or businesses invest more on information security measures, it helps in protecting and lessening loss from cyber risk and failures of the information system Bojanc and Jerman-Blazic (2008).

According to Carr ,(2003), in this electronically world , firms are encouraged to look at how important it is to manage various risk on IT component because at any time when accounting data is changed or erased intentionally or mistakenly , it can cause disorder in the organization whereby there will be suspicious about the data by the users about the reliability and accuracy of the data, therefore it better to manage various risk related to IT component than to apply it for competitive advantage. In the information society, a rational decision maker will invest more on information security if the cost of investing on information security is less than the risk or loss to be incurred, or on the other hand if the investment has another positive return for the company Sangmi et al (2011). Business continuity can be affected by computer incident and the cyber threats which can be a serious problem if not handled and managed on time Gordon, Loeb, Lucyshyn (2005). The incidences may be service denial, telecom fraud, illegal admittance to information, virus, monetary fraud, insider abuse of net access, and system infiltration. To precisely measure the impact and cost of information security investment, it will be ideal for firms to look at possibility of the risk and chances of occurrence as well as the consequences of the information security risk which can be caused by the information system not being secured. CISSP Forum (2007).

The problem of measuring the cost and benefit of investing on information security has been one of the problem why companies don't allocate their resources to information security. Determining the precise expanse of return on information security investment (ROSI) is continually inspiring due to inadequate data for calculating the prospect and rate of information security risk features. The precise estimate of security advantage is a key factor in performing the security economic analysis for effective security investment decision making, the benefit and cost estimation for a security investment is essential Boehm and Survillan (2000).

Gordon and Loeb (2006), the cost of information security can be calculated by the capital or operating expenditure on hardware, software, and personnel. Though, many security managers make a decision based on their experience, judgment, and their best knowledge because the benefit estimation for security investment has been difficult to determine due to a lack of historical data, a lack of effective metrics, and the complex and sensitive nature of security. Several studies suggest using cost benefit analysis for operative information security decision making (Butler, 2002, Flechais et. al 2003, Gordon and Loeb 2006, Kim and Lee 2005). Operative security investment decisions can be made and built on the enquiry of predictable harm from an information security risk and the benefits of information security investment which arises from the efficiency of the countermeasure of security susceptibilities and breaches as well as avoiding imminent loss by mitigating information security risks.

Kim and Lee (2005) suggested in their study, cost and benefit factor analysis in which return on investment (ROI) can be used to compute information security investment. a research also by Ranganathan and Brown (2006), Sabherwal and Sabherwal (2005) confirms that a public announcement by the firms on the IT-based information management and the Enterprise Resource Planning (ERP) plan investments also made a significant positive market response for the firms.

INFORMATION SECURITY INVESTMENT IMPACT ON FIRM PERFORMANCE

As today's businesses and organizations are faced by the increasing rate of cybersecurity threat, it is becoming mandatory for all businesses and organizations of various categories to realize the potential impact of information security vs organizational performance (Ranjit and Xin 2014). Firms will be unprotected from the risk of loss of customers, loss of goodwill and financial penalties amongst others if they don't implement necessary security safeguard to ensure and protect confidentiality, integrity and availability of their information (Karnja and Zaveri, 2014). Organizations today face serious peril because of speedy rise in both capacity and occurrence of nasty attack on their information technology infrastructure. Therefore, firms and businesses have to take an active process to information security development, governance and control, also the allocation of resources to secure the firms information must be tied down to the bottom line and the businesses objectives rather than just on technological structures only (Kwon and Johnson,2014). Firms are also required to control the organizational risk of various

security attack before the occur by allocating resources ensuring understanding the different key security technology investment of factors relating to IT and non IT related and understanding the impact of such investment on organizations.

Bojanc and Jerman-Blazic (2008) states that continuous investments in information security dealings lessen losses from cyber threats and information system failures. Also, information security is a continuing application, demanding constant valuation and enquiring to recognize close susceptibilities earlier before they occur. Prevention, monitoring, and analysis are the important business mechanisms of a robust information security governance that is proficient of enduring all sorts of organizational threat Ranjit and Xin (2014). Few examples of information security technology are: intrusion detection systems, firewalls, encryption, biometric and other authentication devices.

According to Ranjit and Xin (2014), there is no standard measurement that is widely accepted for the firm performance because of the intricate state of businesses currently which makes it makes it incredible to measure firm performance with a sole metric, numerous scopes are required to effectively apprehend it. Thus, there is no any accepted measure for firm's performance in relation to their peers. from the above-mentioned tasks of measurement, the accounting measures, market and the hybrid are the three classes agreed and used by the practitioners and researchers which they said financial measures offers the basis for firm's performance measurement which are frequently used nowadays. Sales growth, return on asset(ROA), Return on equity (ROE), Return on investment (ROI), Return on Sales (ROS), Return on capital Employed (ROCE), are usually the accounting measures of firm's performance.

PERFORMANCE MEASURES AND ACCOUNTING INFORMATION SYSTEM

The successful implementation of AIS has not been adequately researched by the current literature because there is no enough proves to show the relationship between AIS and measurement of performance. The organizations can be impacted positively if they will adapt to the changes in the environment, if the firm's transaction will be managed properly, and a high step of attractiveness and competitiveness Grande et al (2011). According to Ogah, (2012), accounting systems used by organizations does not determine their profit, he noted that other factors also may be looked upon which can add to the bank's profitability, because the adoption of AIS alone without backing it with essential and aiding environment and services will make it less valuable in which the impact will not be appreciated and will also affect the operation process by the banks.

Therefore, the AIS positive integration will rely heavily on how other factors are being used or considered to make sure it has a good impact or the desired goal is achieved. Hence, for AIS to be efficiently operated and successfully integrated other factors must be looked upon which facilitates the operations in which Markus and Pfeffer (1983) gave a similar opinion by saying , for AIS to be successful implemented , some important factors need to be considered which are, how the organization will remark the new technology that is their perception,, secondly is the system of accounting have to suit when problems are normally resolved i.e. the organization' technology, lastly, the accounting system must be suitable with the culture, i.e. the customs and value system that portray the organization. AIS can only become significant in an organization when other factors are looked upon and functioned accordingly Grande et al., (2011). They argued that the availability of IT does not guarantee improved profitability, performance or competitive advantage because so many firms have not succeeded in attaining desired goals after investing in IT.

In a research carried by Ranjit and Xin (2014) on investigating the impact of security investment in which they suggested that a holistic approach must be used to analyze security investment in which different factors must be combined such as the financial, technical, policy and legal. A holistic approach was used in their study in which they identified the critical factors of security investment and their effect on the performance of firms. The researchers used the table below gotten from Intel IT Carty et al (2012) which the table 1 provides non relating factors to IT which include legal and policy, and it was described briefly, most of them have been used to signify the technical insight of security investment. The table 2 provide the factors relating to IT and it was also explained briefly.

TABLE 1 - SECURITY INVESTMENT FACTORS – NON - IT RELATED

FACTORS	BRIEF EXPLANATION
Policies and standard	To protect the confidentiality of customer information, strictly comply with regulations and maintain a security baseline that is above the industry benchmark. The emphasis is on three essential components: Prevention-to employ multi-tiered security solution/environment to contain and limit ant attacks that occur, monitoring- to identify new vulnerabilities, and analysis – of how data is used and assed including employee behaviors.
Risk assessment and management	A function of measuring and mitigating business risk, Tactic for measuring and evaluating information security risk involve determining overall financial impact of a breach- response cost, notification cost, damage to reputation and regulatory files.
Security awareness/education and training.	Security training and education for security awareness aims to make employee aware of security policies and practices and to build a security conscious culture.
Physical security	Includes physical access control for data centers and site security- theft of physical asset, tempering and sabotage
Regulatory compliance	Aims to control compliance cost of a firm for adhering to laws regulation, guidelines and specification relevant to its business.
Insurance and cyber security	The cost value of cyber security insurance coverage which is designed mitigate losses from variety of cyber incidents, including data breaches, network damage and cyber extortion.
Security personnel	Cost of hiring and retention of qualified and certified information security professionals.

TABLE 2 - SECURITY INVESTMENT FACTORS – IT RELATED

FACTORS	BRIEF EXPLANATIONS
Network security	Relies on layers of protection and consist of multiple components including network monitoring and security software in addition to hardware and appliances
Platform security	Platform refers to the underlying hardware and software for a system. platform security is a security models that protects an entire platform and secure the entire span of software or device on that plat form, removing the need to incorporate individual or multiple security measures for different programs on the system.
Application security	Uses software, hardware, and procedural methods to protect application s from external threats helps identify, fix, and prevent security vulnerabilities in any kind of software application irrespective of the function, language or platform.
Mass storage security	Refers to a permanent peripheral storage of large amount of data in persistent and machine readable form using devices or such types of libraries. USB drives, hard disk drives, magnetic tape drive and optical drives
File and data security	Refers to protecting files and data bases from destructive forces and the unwanted actions of unauthorized users.
Response to security attack/breach	Incident response in an organized approach to addressing and managing the aftermath of a security attack/breach. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.
Mobile security	Refers to enterprise wide protection to secure mobile devices and data with integrated device management and consumerization of IT- employees who bring their own devices to the work place for the use of connectivity on corporate networks

Conclusion

From the study, it was discovered by the researchers that in this technology networked world, all firms are encouraged to look at the information security of their organization as a very important aspect in which they need to protect it strongly from cyber threat and computer incident, because it can cause a lot of havoc when any of their information is being tempered with. Organizations are advised to look at the information security planning and governance as a proactive approach in protecting their information because accounting systems need to be kept safe and secured at any moment as it contains sensitive and confidential information. Thus, protecting the

information of any organization should be a major issue which should be attached to the business goals of organization in which resources should be allocated to, rather than just on technological factors.

Information security investment can be weighed by a rational decision maker by looking at the benefits of such investment, that is if the risk of loss will be greater than the cost of investment or if there will be positive returns for the company for such investment which may emerge from the usefulness of the prevention of security susceptibilities and threat, and also by preventing future loss by improving information security

It was also discovered that the qualitative characteristic to make any accounting information system efficient is when it has a sound internal control which Marshal and Romney (2015) asserted that an orderly and efficient conduct of accounting transactions can be achieved when there is a sound internal control which will lead to a better operating efficiency and will result in better financial information reliability for corrective decision making. Accordingly, if organizations can regulate their technology systems of internal control, they can confirm the reliability of their financial report process and improve their control measures (Hoitash and Bedard 2009).

Therefore, this research will be of great important to the management of organization, or various businesses by creating awareness on the usefulness of having proper internal control system by keeping and maintain appropriate, reliable and complete records using accounting information system for decision making, and effective control and planning of their business activities.

The research can also improve the readers' knowledge and the academicians by serving as a reference material and also for further research for those interested in the area of accounting information system or security of the firm's information. The researchers will also like to encourage further research on the measurement of impact of investment in firms' information security on firm's performance.

Acknowledgement

The corresponding author who is a PhD student in University Malaysia Sarawak will like to thank and acknowledge the University for the Conducive Environment of learning and research, my supervisor who is also a co- author, for her advice and guidance, and other co – authors for their contributions. The authors also appreciate the effort and time of the reviewer(s).

REFERENCES

Akpan, E. S., & Riman, H. B. (2012). Does corporate governance affect bank profitability? Evidence from Nigeria. American International Journal of Contemporary Research, 2(7), pp 135-145.

Beynon-Davies, P. (2002) Information System: An Introduction to Informatics in Organizations, 1st edn. New York: Palgrave, pp 40-44.

Bhagat, S., & Bolton, B. (2008). Corporate governance and firm performance. Journal of Corporate Finance, 14, pp 257-273.

Bhardwaj, A.S., Bharadwaj, S.G. & Konsynski, B.R. (1999). Information technology effects on firm's performance as measured by Tobins Q. Information system research, Vol.45(6), pp 1008-1021.

Bojanc R., & Jerman-Blazic, B. (2008). An economic modeling approach to information security risk management, an international journal of information management 28(5), pp 413-422.

Bojanc, R., & Jerman-Blazic, B. (2008) Towards a standard approach for quantifying an ICT security investment, computer and standard interface 30(4), pp 216-222.

Borthick, A. F., & Clark, R. L. (1990). Making accounting information systems work: An empirical investigation of the creative thinking paradigm. Journal of Information Systems, 4(3): pp 48-62.

Butler, S.A. (2002). Software evaluation: security attributes evaluation method: a cost benefit approach. The 24th international conference on software engineering.

Carr N. (2003). IT doesn't matter. Harvard Business Review 81(5), pp 41-49.

Carty, M., Pimont, V. and Schmid, D.W. (2012), "Measuring the value of information security investment", IT @Intel white paper, Intel Corporate, Santa Clara, CA.

CISSP Forum (2007). i.k.i.s forum Top information security risks for 2008 in C.p.b.p.i.s communities (Ed), pp 1-8.

Flachais A.I., A. Sasse, S. Hailes (2003). Bringing security home: a process for developing secure and usable systems, The workshop on new security paradigms. ACM Press, Ascona, Switzerland, pp 49-57.

Gordon, L. & Loeb, M. (2006). Budgeting process for information security expenditure, communications of the ACM 29(1) pp 121-126.

Gordon, L., Loeb, M., & Lucyshyn, W. (2005). The annual CSI/FBI computer crime and security survey, in: CSI (Ed.), pp 26.

Grande, U. E. Estebanez, P. R. & Colomina, M.C (2011). The impact of accounting information on performance measures: empirical evidence in Spanish SMEs. The international journal of digital accounting research, 11 (2011), 25-43.

Haddad, & Atmeh. (2009). Accounting information system (1st Ed.). pp 43. Amman: Al Mareekh.

Holden, K. and El-Bannany, M. (2004) Investment in information technology systems and other determinants of bank profitability in the UK, Applied Financial Economics, 14(5), 361365

Hoitash, U., Hoitash R. and Bedard, J.C. (2009): "Corporate governance and internal control over financial reporting; a comparison of regulatory regimes," Account. Rev., 84(3), pp. 839-867.

Hussani and kharabsheh (2000). Requirement of financial controlling department on performance controlling. administrative sciences journal 27(2), pp 34-56.

Ismail, N. A., and King, M. (2005). Firm performance and AIS alignment in Malaysian SME´s. International Journal of Accounting Information Systems, vol. 6, n.4, P. 241-259.

Kim, S., & Lee, H, (2005). Cost-benefit analysis of security investment; methodology and case study, ICCSA 2005, LNCS, 3482, pp 1239-1248.

Kuranga, E. & Zaveri, J. (2014). Ramifications of the Sarbanes Oxley (SOX) Act on IT governance. International journal of accounting and information management, 20(2), pp.134-145.

Kwon, J. & Johnson, M.E. (2014). Proactive versus reactive security investment in the healthcare sector. MIS Quarterly, 38(2), pp 227-240.

Laudon, K.C & Laudon, J.P (2005) Essentials of Management Information Systems, 6th edn. New Jersey: Prentice Hall.

Laudon, K.C. & J.P. Laudon, 1991. Managing information systems: A contemporary perspective. 4th Edn.: New York: Macmillan

Loch, K., Carr, H., Warkentin M. (1992). Threat to information systems: today reality, Yesterday's understanding MIS quarterly 16(2), pp 173- 186.

Markus, M. L., & Pfeffer, J. (1983). Power and the design and implementation of accounting and control systems. Accounting, Organizations and Society, 8(2), 205-218

Marshal, B.R & Paul J.S. (2015): Accounting Information Systems. Thirteen Edition. Pearson Education Limited. pp 214-234.

Melinda, K. & Stephen, C. (2001) A Study of the Information Technology Investment on Firm Performance, Journal of Computer Information Systems, 41(3), pp 5-15.

Ogah, I.J. (2012). An evaluation of the relevance of accounting system as a management decision tool in Union bank of Nigeria PLC. Uyo branch of Akwa Ibom Greener. journal of business and management studies 3(1), pp 38-45,

Oguntmehin, A (2001): Teacher effectiveness; Some practical strategies for successful implementation of universal basic education in Nigeria, African Journal of education management, 9(1) pp 151-161.

Pérez, R., Urquía, E., & Muñoz, C. (2010). Information technology implementation: evidence in Spanish SMEs. International Journal of Accounting & Information Management, 18(1), pp 39-57.

Pérez, R., Urquía, E., & Muñoz, C. (2010). Information technology implementation: evidence in Spanish SMEs. International Journal of Accounting & Information Management, 18(1), pp 39-57.

Poudel, R. P. S., & Hovey, M. (2013). Corporate governance and efficiency in Nepalese commercial banks. International Review of Business Research Papers, 9(4), 53-64.

Qatawneh, A. (2005). The effect of using information technology of accounting information system efficiency. Unpublished PhD thesis. Arab Academy for finance and banking.

Ramly, F. (2011). Computerize Accounting Information System. Decision making 16(1), pp 12-31.

Ranganathan, C., Brown, C. (2006). ERP investment and the market value of firms: Towards an understanding of influential ERP project variables information systems Research vol 17, pp 145-161.

Ranjit, B. and Xin L. (2014). Investigating security investment impact on firm performance. Accounting journal of accounting and information management 22(3), pp 194-208.

Razak, N. H. A., Ahmad, R., & Joher, H. A. (2011). Does government linked companies (GLCs) perform better than non-GLCs? Evidence from Malaysian listed companies. Journal of Applied Finance and Banking, 1(1), 213-240.

Romeney, B., & Steinbart, J. (2003). Accounting information systems. prentice hall business publishing (9th Ed), pp 58-66

Sabherwal, R., & Sabherwal S. (2005). Knowledge management using information security: determinant of short term impact on firm value, Decision sciences 36(4) pp 531-568.

Chai, S., Das, S., & Rao, H. R. (2011). Factors affecting bloggers' knowledge sharing: An investigation across gender. Journal of Management Information Systems, 28(3), 309-342.

Shaheen, A. (2012). Factors affecting accounting information system efficiency Islamic University Gaza.

Topash, N.K (2014).: Evaluation of Efficiency of Accounting Information Systems: A Study on Mobile Telecommunication Companies in Bangladesh. Global Disclosure of Economics and Business, 3(1), pp 40-55.

Wilkinson, J. W. (1993). Accounting Information Systems: Essential Concepts and Applications. Second Edition. New York: John Wiley & Sons Inc. pp22-28

Wilkinson, J.W., Cerullo, M.J., Raval, V. & Wong-On-Wing, B. (2000). Accounting Information Systems: Essential concepts and Applications. Network: John Wiley and sons, pp 31-36

Wynn, M. & Maldonado, G. (2007) Implementing Enterprise Resource Planning (ERP) Systems through Knowledge Transfer Partnerships: Two Case Studies, International Journal of Management Cas es, 9(2), pp 41-51.