

**Information Assurance Strategies and Organizational Performance of Government Hospitals in Rivers State, Nigeria**

---

**Anthonia E. Bestman, PhD.**  
tonianestman@gmail.com

And

**Maurice E. Ikuru**  
Department of Office and Information Management  
Rivers State University  
Port Harcourt.

---

**Abstract**

This study examined the relationship between information assurance strategies and organizational performance of government hospital in Rivers State. The objective of the study was to examine how the dimensions of information assurance strategies such as risk-based approach influence the measures of organizational performance such as growth and task delivery. The study adopted a cross-sectional survey in its investigation of the variables. Primary source of data was generated through self-administered questionnaire. The population of this study was 190 employees of three (3) selected government hospital in Rivers State. The sample size of 130 was drawn using the Taro Yamane sample size determination formula. Data were collected using the four (4) Likert type scale, data were analyzed and the hypotheses were using with the use of Spearman rank order correlation coefficient statistics with the aid of statistical package for social sciences (SPSS). The study findings revealed that there is a positive significant relation between the dimension of information assurance strategies and organizational performance of government hospital in Rivers State respectively. Therefore, the study recommends that public hospitals should consider the strategic data class; integrate it as a culture of the organization.

**Keywords:** *Information Assurance Strategies, Organizational Performance*

**1. Introduction**

Information is as old as nature, it preceded the existence of man, it plays key role in shaping and enhancement of civilization, especially as it concern organizations, families, communities, nations and the world in general, in our modern society. It assumes the form of both formal and informal conversation, meetings, telephone calls, personal conversation, letters, reports, memos and trade publications. Hardly can any organization or system perform efficiently without information.

Information is seen as amorphous and can be printed on paper, stored on computers, sent by post or electronically, shown on videos and articulated in a discussion (Von Solms and Van Niekerk 2013). As well as being stored on physical media such as the newspaper and digital media such as computers, information can also reside on cognitive media, i.e. people's minds (Ahmad, Ruighaver & Teo, 2005). Information can also have various levels of sensitivity, it is difficult to control which sometimes results in leakage, and is intangible in nature (Ahmad et al. 2005). Information however is not data, with the distinction being that data are raw facts and information is processed data that is meaningful (McKinney Jr and Yoos 2010). It is interesting to note that information hosted in the cloud brings its own set of challenges including: long-term viability, where information restoration becomes doubtful should the cloud vendor become bankrupt, and information availability, where cloud vendors may not restore to a different environment should the information become unavailable (Catteddu 2010).

Information Assurance (IA) is quite a new discipline, perhaps, the most striking feature of which everyone seems to have different opinion about what it actually is, in order to understand the meaning of IAS, First, the understanding of the term based on common English is examined. Then,

we present the analysis of the definitions of IAS provided by the official organizations, followed by the analysis of the comprehension of the discipline in the academic and industry publications. The Oxford English Dictionary (2012): Assurance is a positive declaration intended to give confidence; a promise; Confidence or certainty in one's own abilities.

Confidence is defined as "the feeling or belief that one can have faith in or rely on someone or something, according to Oxford English Dictionary, 2012. Based on the "distilled knowledge and wisdom embodied in the dictionary definitions", (Sherwood et al., 2005) coin a general definition of IAS: Information Assurance Strategies is a discipline the main aim of which is to give confidence or certainty in information; to give belief that one can rely on data, knowledge, facts, and its meaning.

One important assumption that comes out of the above definition is that confidence in information must be based on confidence in all entities involved in the processes of information processing, storage and transmission. An entity, in this context, may mean a technical tool or system, a process, an individual or an organization. Information Assurance as defined in the official US and UK documents, the term IA was coined by the US Joint Staff\_ in 1998 and for the \_first time appears in Joint Doctrine for Information Operations (Joint Pub, 1998).

This document provided the classical definition of IA that for the \_first time declared \_five security goals, also known as the Five Pillars of IA: availability, integrity, authentication, confidentiality and non-repudiation. Information assurance (IA) is the process of ensuring that the right people get the right information at the right time. Culture has influenced the formation of many information assurance measures, such as the national security policy, information ethics, security training, and privacy issues (Chen, Medlin, & Shaw, 2008). Information assurance culture covers social, cultural and ethical measures to improve the security relevant behavior of the organizational members and considered to be a subculture of organizational culture (Schlienger & Teufel, 2002). Security culture should support all organizational activities in a way that information assurance becomes a natural aspect in the daily activities of every employee (Schlienger and Teufel, 2002).

Griffin (1996) states that in the management of an organized system, information are closely linked or related since management is conceptualized as a series of steps involving the reception, processing and dissemination of information; he further observed that information is vital to the daily operations and strategic management of an organization.

With the introduction of networks and increase in internet information assurance, industries are increasing the ratio it network-based service, with such development operator are to grasp the importance of information assurance practices.

Information assurance (IA) is an area of interest since information is seen as a key asset by many organizations. Organization pay increasing attention to information protection also because the impact of information assurance breaches today have more tangible, often devastating effect on business (Dlmini et al , 2009).

However, organizational performance is mostly measure with financial indication on investment. Didier Noye (2002) believes that the performance consists of "achieving the goals that were given to you in convergence of enterprise orientations" In his opinion, performance is a mere finding of an outcome, but rather it is the result of comparison between the outcome and the objective. Bartoli

and Blatrix's opinion (2015) performance should be achieved through items such as evaluation, piloting, efficiency, effectiveness and quality. Therefore, organization should see information assurance as part of the tools that will enhance task delivery and organizational growth.

Meanwhile, managers tend to put their attention to the results that are valued by the board of directors (Finkelstein & Hambrick, 1996). That is, if their own performance is assessed with the profitability criterion or the profit per share, they would tend to score well on this criterion. As Tom Peters noted: "what gets measure, gets done". Managers who stick too closely to the financial performance indicators tend to adopt a lean management system. Managers who are solely interested in financial performance not only adopt a short term perspective that can be harmful to the organization durability, but they also may be harmful to the other stakeholders (DeBusk & al., 2003; Beu & Buckley, 2003). The short term perspective is a vicious circle which could lead to the disintegration of the organization.

Organizations are formed with the combination of animate and inanimate. Thus. In order to achieve quality performance attention to critical things like data arrangement, information system, information security and availability must be monitored by top management. Although, many studies have found that different companies in different countries tend to emphasize on different performance measurement, but in this study we suggest task delivery and organizational growth.

Compliance processes help organizations compare their actual information assurance operations with international IAM standards (Karabacak & Sogukpinar, 2006). Compliance evaluates and audits the difference between the expected standards of organizational situations, and the reality in the organization (Karabacak & Sogukpinar, 2006). Evaluating the degree of compliance helps organizations determine their conformity to the controls listed in the standards, and delivers useful outputs to the certification process for the next stage of IAM certification (Karabacak & Sogukpinar, 2006). Compliance with internationally recognized standards is growing in importance, because it has become popular as a common basis for information assurance measurement (Karabacak & Sogukpinar, 2006).

It is therefore important for organizations to be able to evaluate their information assurance compliance level (Karabacak & Sogukpinar, 2006; Luthy & Forcht, 2006; Saleh, Alrabiah & Bakry, 2007). Compliance levels increased in organizations that were more aware of their IAM issues, which could lead to improved information security policy and business continuity plans in their organizations (Smith, Jamieson, and Winchester, 2007). Unfortunately, many organizations cannot distinguish between information assurance compliance management and information assurance operational management (von Solms, 2005). There have always been problems for organizations in term of information assurance compliance, which is an obstacle that needs to be overcome in order to achieve the benefits of IAM. As a result, there is a need to find a method to ensure that the practices of employees are compliant company information assurance policies (Vroom, R. von Solms 2004), particularly because a significant number of security breaches result from employees' failure to comply with security policies (Beautement, Sasse, and Wonham, 2008). Many organizations have tried to change or influence security behavior, but found it a major challenge (Beautement, et al., 2008). Thus, adherence to strategies is important to goals achievement. This study sought to fill the existing research gap by examining the relationship between information assurance strategies and organizational performance of government hospital in Rivers State.

This study will also be guided by the following specific objectives:

- i. Ascertain the extent to which risk-based approach relates with growth of government hospital in Rivers State.
- ii. Ascertain the extent to which risk-based approach relates with task delivery of government hospital in Rivers State.

## 2. Theoretical framework

### 2.1. The Network Society Theory

Manuel Castells' groundbreaking trilogy, *The Rise of the Network Society* (1996,1997, 1998), exemplifies a 'technological' approach to globalization. While his theory shares with world-system and global capitalism approaches an analysis of the capitalist system and its dynamics, it is not the logic of capitalist development but that of technological change that is seen to exercise underlying causal determination in the myriad of processes referred to as globalization. Castells' approach has been closely associated with the notion of globalization as representing a new 'age of information'. In his construct, two analytically separate processes came together in the latter decades of the twentieth century to result in the rise of the network society. One was the development of new information technology (IT), in particular, computers and the Internet, representing a new technological paradigm and leading to a new 'mode of development' that Castells terms 'informationalism'. The other was capitalist retooling using the power of this technology and ushering in a new system of 'information capitalism', what Castells and others have alternatively referred to as the 'new economy'.

This new economy is: (1) informational, knowledge-based; (2) global, in that production is organized on a global scale; and (3) networked, in that productivity is generated through global networks of interaction. Castells' definition of the global economy is an 'economy with the capacity to work as a unit in real time, or to choose time, on a planetary scale', and involving global financial markets, the globalization of trade, the spread of international production networks, and the selective globalization of science and technology. A key institution of this new economy is the 'networked enterprise', which Castells sees as the vanguard of a more general form of social organization, the network society itself. This involves a new organizational logic based on the network structure in interaction with the new technological paradigm. The network form of social organization is manifested in different forms in various cultural and institutional contexts. Here Castells, along with global capitalism approaches, that of Harvey (see below), Lash and Urry (1987), Cox (1987), and others, draw on a number of strands of late twentieth-century political economy scholarship, especially that of post-Fordism and flexible accumulation, involving a breakdown of the old rigid, vertical corporate structures and the rise of new horizontal and flexible structures. In Castells' view, 'the networked enterprise makes material the culture of the informational, global economy: it transforms signals into commodities by processing knowledge' (1996: 188). Castells goes on to argue that the image of giant transnational corporations (TNCs) as centralized structures driving the global economy is 'outdated' and 'should be replaced by the emergence of international networks of firms and of subunits of firms, as the basic organizational form of the informal, global economy' (1996: 206–7).

### **3. Concept of Information Assurance Strategies (IAS)**

Information Assurance Strategies is an area of interest especially in social science, (Stone burner & Alexis, 2002) opine that an information assurance policy is a combination of principles, regulations, methodologies, techniques and tools established to protect the organizations information from threats. These policies also help organizations to identify its information assets and define the corporate attitude to these information assets (David, 2015).

Protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Information systems security (INFOSEC): In contrast cost-related strategic performances focus on standardization and comparability of activities and processes (Naranjo-Gil & Hartmann, 2006), which demands the use of a narrow set of information, which expresses cost control objectives in financial (monetary) and aggregated terms (Choe, 1996), facilitating comparability of tasks and outputs across the organization (Chang, Chang, & Paper, 2003, Kyung, 1990). As society increasingly relies on digitally stored and accessed information, traditional information security technologies, policies, management and practices are found more and more limited in satisfying the assurance needs of modern information systems and applications, for several reasons. In general, addressing only the protection of information against unauthorized disclosure, transfer, modification, or destruction, traditional information assurance strategy cannot deliver the level of information assurance that modern applications require base on the numerous challenges the present firms are facing.

These attacks can cause substantial confidentiality and privacy loss (via unauthorized disclosure of information), substantial integrity loss (via unauthorized modification of information), substantial availability/reliability loss and serious denial of service (via destruction of some critical components of the information system), and substantial non-repudiation loss (via destruction of evidence and audit data). When applications were lightly dependent upon digitally stored and accessed information, such information security losses might be able to be tolerated. But as applications increasingly rely on digitally stored and accessed information, such security losses can be disastrous and may no longer be able to be tolerated. Hence, another fundamental limitation of traditional information security is that how to address these successful attacks, or intrusions. As a result, to meet the security and assurance needs of modern information systems and applications, a broader perspective is introduced, saying that, in addition to preventing information from being disclosed, modified or destroyed, intrusions should be detected; countermeasures (e.g., responses) to intrusions should be planned and deployed in advance; security and fault tolerance mechanisms should work together to ensure confidentiality, privacy, integrity, non-repudiation, authenticity, availability and reliability in the presence of attacks; and the damage caused on the information and the information system should be repaired and restored (or recovered).

### **4. Concept of Organizational Performance**

The word ‘performance’s is derived from the word ‘performance’ which mean ‘to do’ ‘to carry out’ or ‘to render’, it refer to the act of performing, execution, accomplishment, fulfillment, etc. In broader sense, performance refers to the accomplishment of a given task measured against preset standard of accuracy, completeness, cost and speed (Kohlar, 2015). In other words, it refers to the degree to which an achievement is being or has been accomplished. The word of Kohlar (2015), the performances a general term applied to a part or to all the conducts of activities of an organization over a period of time often with reference to past or projected cost efficiency,

management responsibility or accountability or the like. Thus, not just the presentation but the quality of result achieve over a given period of time and can be use to compare similar firms across the same industry or to compare industries or sectors in aggregation. The study of organizational performance holds a central position in the management of private and public organizations as well as in the field of organizational research. Over the last decades, concerns for efficiency, productivity, excellence and total quality have become increasingly widespread in Western organizations (Lewin & Minton, 1986). These concerns are often motivated by the perception of threats to the durability of the organization. They also seem to be justified by the ever-greater international competition for market shares and resources (Maltz, Shenhar & Reilly, 2003).

## **5. Measures of Organizational Performance**

### **5.1. Growth**

As organization desire to grow and increase especially as it is one means to measure her performance, the word growth is seen differently from different people, the terms “growth” and “development” are frequently used interchangeably but both of the concepts refer to different processes in natural and social systems. According to Encyclopaedia Britannica ”growth is an increase in the size or the amount of an entity” whereas development encompasses change not only in the size but also in the function. Growth is generally associated with a quantitative external change, hence it’s easy to observe and measure. The relationship between business growth and development is an interesting area for research and study. It is expected that the relationship can be multifold. The two may reinforce each other (Aktouf, 1982) when the physical growth of the company in terms of sales or number of employees is accompanied by increased excellence in management, innovation and pursue of learning. The two may also be in conflict when a growing company neglects the need of renewal and change. Then growth may be accompanied by decrease in effectiveness, productivity or creativity. This is what Peter Drucker calls a wrong kind of growth (Drucker, 1980) and would mean lack of development.

### **5.2. Task Delivery**

Delivering of task or services of high quality is an important pursuit for service providers that seek to provide value to their customer (Gronroos and Ravald, 2011). Through the provision of high levels of service quality, companies can achieve increased customer satisfaction, loyalty and therefore long-term profitability (Zeithaml and Bitner, 2000). In a services management context, service delivery system is defined as “ the structure (facilities, equipment, etc.), infrastructure (job design, skills, etc.) and processes of delivering a service” (Goldstein et al. 2002). From the definition it become apparent that SDS effectiveness is related to the degree to which a system’s objectives is have been achieved and therefore, an effective SDS is the one that is capable of delivering the outcome for which it was originally design and developed (Kilbourne, Duffy, Duffy & Giarchi, 2004). To deliver high-quality, reliable, and consistent services safely, organizations develop professional standards. These standards may be adopted from external agencies (e.g., professional industry groups, external regulators) or developed through the internal documentation and proliferation of best practices. There are often significant benefits associated with adopting professional standards. For instance, within health care, implementing a 19-item surgical safety checklist recommended by the World Health Organization (WHO) was found to reduce the rate of deaths and inpatient complications by 47% and 36%, respectively (Haynes et al., 2009). As such,



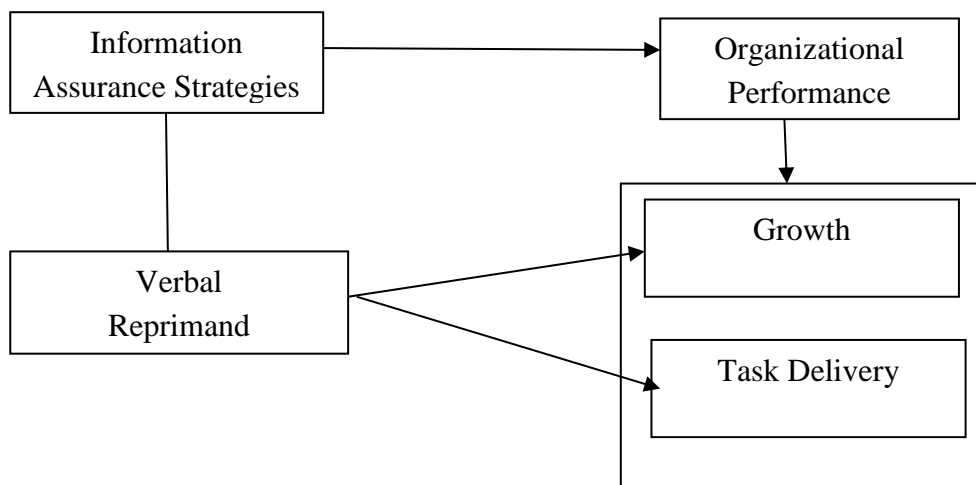
the importance of complying with professional standards is frequently communicated, and actual compliance is reinforced and rewarded within organizations.

## 6. Risk Based Approach and Organizational Performance

The important of risk based approach in a firm cannot be overemphasize, because it deals with the protection if information which is a very valuable asset against threat. All organization makes use of data for her activity which is geared towards achieving workplace goal, activities in a way that information security becomes a natural aspect in the daily activities of Culture has influenced the formation of many security measures, such as national security policy, information ethics, security training, and privacy issues (Chen, Medlin, & Shaw, 2008). Security culture covers social, cultural and ethical measures to improve the security relevant behavior of the organizational members and considered to be a subculture of organizational culture (Schlienger & Teufel, 2002). Security culture should support all organizational aevery employee (Schlienger and Teufel, 2002). Organizations engages in risk based approach because it enable her to keep track of all her information which will in turn lead organizational to efficiency.

From the foregoing point of view, we hereby hypothesized thus:

- H<sub>01</sub>** There is no significant relationship between risk based approach and task delivery of government hospital in Rivers State.
- H<sub>02</sub>** There is no significant relationship risk based approach organizational growth of government hospital in Rivers State.



**Fig.1** Operational framework for the hypothesized relationship between information assurance strategies and organizational performance

*Source: Author's Desk Research, 2018*

## 7. Methodology

The study adopted a cross-sectional survey in its investigation of the variables. Primary source of data was generated through self-administered questionnaire. The population of this study was 190 employees of three (3) selected government hospital in Rivers State. The sample size of 130 was drawn using the Taro Yamane sample size determination formula. Data were collected using the

four (4) Likert type scale, data were analyzed and the hypotheses were using with the use of Spearman rank order correlation coefficient statistics with the aid of statistical package for social sciences (SPSS).

## 8. Results and Discussions

### 8.1. Bivariate Analysis.

Data analysis was carried out using the Spearman rank order correlation tool at a 95% confidence interval. Specifically, the tests cover a Ho1 hypothesis that was bivariate and declared in the null form. We have based on the statistic of Spearman Rank (rho) to carry out the analysis. The level of significance 0.05 is adopted as a criterion for the probability of accepting the null hypothesis in ( $p > 0.05$ ) or rejecting the null hypothesis in ( $p < 0.05$ ). We will begin by presenting first a test of existing relationships.

Table 1: Correlations Risk-Based Approach and Measures of Organizational Performance

Measures		Risk-based approach	Task delivery	Growth	
Spearman's r	Risk-based approach	Correlation Coefficient	1.000	.938**	.902**
		Sig. (2-tailed)	.	.000	.000
		N	130	130	130
	Task delivery	Correlation Coefficient	.988**	1.000	.633**
		Sig. (2-tailed)	.000	.	.000
		N	130	130	130
	Growth	Correlation Coefficient	.902**	.633**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	130	130	130

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

**Ho1: There is no significant relationship between risk-based approach and task delivery in the hospital in Port Harcourt.**

From the result obtained in the table 1 shows that there is positive relationship between correlation coefficient (r) of risk-based and task delivery. The  $r$  value 0.938 prove that the relationship and it is significant at  $p 0.000 < 0.01$ . The correlation coefficient shows a very high correlation indicating also a very strong relationship among the variables. However, based on findings the null hypothesis stated is hereby rejected and the alternate is considered.

**Ho2: There is no significant relationship between risk-based and growth in hospital in Port Harcourt.**

From the result obtained in the table 1, shows that there is positive relationship between correlation coefficient (r) of risk-based and growth the correlation coefficient (r) shows that there is a significant and positive relationship between data classification and growth. The  $r$  value 0.902 prove that relationship and it is significant at  $p 0.000 < 0.01$ . The correlation coefficient shows a very high correlation indicating also a very strong relationship among the variables. Thus, based on findings the null hypothesis stated is hereby rejected and the alternate is considered. Thus, there



is a significant relationship between the risk-based approach and growth of hospitals in Port Harcourt.

## **9. Discussion of Findings**

The study adopted descriptive and inferential method to investigate the relationship between information assurance strategies and organizational performance of hospitals in Rivers State. The finding revealed a significant and positive relationship between information assurance strategies of hospital in Rivers State. That is why (von Solms, 1996) said that it enhances the confidence and effectiveness of information services within the organization or between external parties. Assurance cultures assist the enforcement of information security policies and practices to the organization. As a result, each organization goal's is to be able achieve an effective information security culture in their organization. Information security culture will emerge over time and become evident in the behavior and activities of the workforce (da Veiga, Martins, & Eloff, 2007). From the study it was shown that there is a strong correlation between risk-based approach and organizational performance. Hence the null hypothesis are hereby rejected. Risk-based approach need to be classified to achieve the primary objective; classification of risk is the first step any manager must take before deciding on the method of information security, risk management and control to be taken. (Jan, 2001).

In business studies organizational growth is manifested through increase in the number of employees, income, profit, or market share. These are the measures of externally visible quantifiable changes of the organization. Business development is more difficult to define. It is associated with the process of organizational learning and transformation which are qualitative in nature. "To grow is to increase in size or number. To develop is to increase one's ability and desire to satisfy one's own needs and legitimate desires and those of others. A legitimate desire is one that, when satisfied, does not impede the development of anyone else. Development of individuals and corporations is more a matter of learning than earning" (Ackoff, 1999).

The relationship between business growth and development is an interesting area for research and study. It is expected that the relationship can be multifold. The two may reinforce each other (Ackoff, 1999) when the physical growth of the company in terms of sales or number of employees is accompanied by increased excellence in management, innovation and pursue of learning. The two may also be in conflict when a growing company neglects the need of renewal and change. Then growth may be accompanied by decrease in effectiveness, productivity or creativity. This is what Peter Drucker calls a wrong kind of growth (Drucker, 1980) and would mean lack of development.

## **10. Conclusion and Recommendation**

This study aimed at examines the relationship between information assurance strategies and organizational performances of hospitals in Rivers State. More so, the research strategy and method were carefully designed as such it is geared towards the achievement of the objective of the study. The study also unveiled a positive and significant relationship between the information assurance and organizational performance of hospital in Port Harcourt, which connote that, risk based strategy used by management of the studied hospitals have increased organizational task delivery and growth.

Based on the findings obtained from summary of discussion and empirical findings the following recommendations are made:

1. Information security values should not be played with as it protect against unauthorized users.
2. Organizations administrators should engage in research to enable the organization have information available that are first class information which will lead to best practice

## References

- Ahmad, A., Ruighaver, A., & Teo, W. (2005). An Information-Centric Approach to Data Security in Organizations, TENCON 2005 IEEE Region 10: IEEE.
- Aktouf, O. (1982). Une approche observation participante et intellectuelle des systèmes de représentation dans les rapports de travail. Unpublished Thesis Dissertation, Montréal: École des Hautes Études Commerciales.
- Bartoli A., Blatrix C. ( 2015). Management dans les organizations publiques - 4ème edition Management in Public Organizations - 4th Edition, Dunod, Paris,
- Beautement, A., Coles, R., Griffin , J., Monahan, B., Pym, D., Sasse, M. A., & Wonham M. (2008). Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security. Workshop on Economics in Information Security 2008. 25-28 June, 2008, Hanover, New Hampshire, USA.
- Catteddu, D. (2010). Cloud Computing: benefits, risks and recommendations for information security. *Web Application Security*. Springer, 17-17.
- Chang, R., Chang, Y., & Paper, D. (2003). The effect of task uncertainty, decentralization and AIS characteristics on the performance of AIS: An empirical case in Taiwan. *Information & Management*, 40, 691–703.
- Chen, C.C., Medlin, B.D. & Shaw, R.S. (2008). A cross-cultural investigation of situational
- Choe, J. M. (1996). The relationships among performance of accounting information systems, influence factors and evolution level of information systems. *Journal of Management Information Systems*, 215–239
- Dhillon, G. (1997). *Managing information system security*, MacMillan Press Ltd, Great Britain. 210
- Finkelstein, S. & Hambrick, D. (1996). Strategic Leadership Top Executives and Their Effects on Organizations. West Publishing Company, St. Paul.*

- [Grönroos](#), C., & [Ravald](#), R. (2011). Service as business logic: implications for value creation and marketing. *Journal of Service Management*, 22 (1), 5-22,
- Kilbourne, W. E., Duffy, F. A., Duffy, M., & Giarchi, G., (2004). The applicability of SERVQUAL in cross-national measurements of health-care quality. *Journal of Service Marketing*, 18 (7), 524-533
- [Kingman-Brundage](#), J. (1991). Technology, design and service quality. *International Journal of Service Industry Management*, 2 (3), 47-59.
- Kyung, K. (1990). Task characteristics, decentralization, and the success of hospital information systems. *Information & Management*, 19, 83–93.
- Lewin, A. Y., & Minton, J. W. (1986). Determining Organizational Effectiveness: Another Look, and an Agenda for Research. *Management Science*, 32(5), 514–538.
- Luthy, D., & Forcht, K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security*, 14 (2), 155-166.
- Maltz, A.C., Shenhar, A.J., & Reilly, R.R. (2003). Beyond the balanced scorecard: Refining the search for organizational success measures. *Long Range Planning*, 36, 187-204.
- McKinney Jr, E.H., & Yoos, C.J. 2010. Information about information: a taxonomy of views. *MIS Quarterly*, 34(2), 329-344.
- Naranjo-Gil, D. & Hartmann, F. (2007). Management accounting systems, top management team heterogeneity and strategic change. *Accounting, Organizations and Society*, 32:735-756.
- Saleh, M.S., Alrabiah, A., & Bakry, S.H. (2007). A Stope model for the investigation of compliance with ISO 17799-2005. *Information Management & Computer Security*, 15(4), 283-294.
- Schlienger, T., Teufel, S. (2002). Information Security Culture: The Socio-Cultural Dimension in Information Security Management, Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egypt. IFIP Conference Proceedings 214, pp. 191-202
- Schlienger, T., Teufel, S. (2002). Information security culture: the socio-cultural dimension in information security management, Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egypt. IFIP Conference Proceedings 214, pp. 191-202

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102

von solms, r. (1998). information security management (3): the code of practice for information security management (Bs 7799). *Information Management & Computer Security* 6 (5), 224-225.

Zeithaml, V.A. & Bitner, M.J. (2000). *Services marketing: integrating customer focus across the firm. 2nd edition*. Boston: McGraw-Hill.