IABE® International Academy of Business and Economics®
IABE.eu Promoting Global Competitiveness™
Admin@iabe.eu

Date: MAY, 19, 2014

IABE-2014 VERONA

To: **Aukkaradej Chaveerug**

Re: Your Paper:

ACCOUNTING INFORMATION SECURITY EFFECTIVENESS THROUGH TECHNOLOGICAL FRAMES OF REFERENCE

Dear Author(s),

Congratulations! On conclusion of the double-blind review process, **your paper is accepted for publication** in ***Journal of Academy of Business and Economics***™ (JABE). The JABE is a refereed publication listed in Cabell's Directories 2002-14 Editions and in Ulrich's International Periodicals Directory since 2003. The JABE is available online at the EBSCO Publishing in the Business Complete Listing and at the Gale/ Cengage Publishing. The journal will soon be available with the SCOPUS.

In addition, your paper is accepted for presentation at the IABE-2014 VERONA - Summer Conference, June 27-29, 2014. We invite you to visit our website www.iabe.eu for more information on the IABE, conference registration policy, Online/Email registration, registration form, manuscript submission guidelines, Program Outline, and Conference Hotel information.

Online Registration: Please complete your registration online at **www.iabe.eu** soon. During online registration process, you can pay your applicable fees, upload formatted paper, and **join the IABE as a Full Professional Member**. You may also complete your registration by email using info available online. **At least one author is required to register and pay applicable fee(s) in order to have the accepted paper published.**

Registration Deadline:

Please complete your registration BY MAY 26TH, 2014. Accepted paper submitted late or in non-conforming format or without full amount of applicable fees may not be published. We expect coauthor(s) also to register for and attend the conference.

Copyright: Articles/papers submitted to the journal JABE, should be original contributions and should not be under consideration for or published in any other publication. The author(s) is (are) solely responsible for the contents of the paper(s). Authors submitting articles/papers for publication warrant that the work is not an infringement of any existing **copyright** and will indemnify the AIBE/IABE/publisher or sponsor(s) against any breach of such warranty. For ease of dissemination and to ensure proper policing of use, papers/articles/cases and contributions become the legal copyright of the AIBE/IABE/publisher unless otherwise agreed in writing.

Please feel free to contact me at mgavriletea@yahoo.com , admin@iabe.org

Best Regards,

Marius Gavriletea
Marius Gavriletea, Ph.D.
VERONA, Program Chair

Accounting Information Security Effectiveness through Technological Frames of Reference

Aukkaradej Chaveerug
Mahasarakham Business School, Mahasarakham University, Thailand

ABSTRACT

The objective of this research is to examine on using technological frames of reference (TFR) to study the accounting information security gap created by incongruent perceptions related to information risk. Data collection is done by sending the questionnaires to CFO of Thai-listed firms; measurements of constructs both the validity and reliability use the Ordinary Least Squares (OLS) regression analysis to test the hypotheses relationship and estimate factors affecting the accounting information security effectiveness. The results show the technological frames of reference (nature of information security, use of information security, information security strategy) has positive relationships with reduced accounting information security incongruity and reduced accounting information security incongruity has positive relationships with accounting information security effectiveness. Theoretical, managerial and research implications are also discussed.

Keywords: *Technological Frames of Reference (TFR), Nature of Information Security, Use of Information Security, Information Security Strategy, Reduced Accounting Information Security Incongruity, Accounting Information Security Effectiveness*

1. INTRODUCTION

Accountants have the accounting information system knowledge; accountants can to skill or expertise and knowledge of accounting process about understand and analyze the concentration of controls in an electronic environment; understand information systems and understand the use of computer accounting software. It includes information technology based resources deployment as knowledge assets and physical information technology infrastructure (Yang and Guan (2004). Information security has evolved to include organizationally focused methods (Dhillon, G. and Backhouse, J. (2000). Advancement in technology has created significant risk implications on accounting information systems. The underlying technology appears to develop faster as compared to the relative advancement in control practices which had not been combined with professional accountants' knowledge, skills and attitudes in the use of computing technologies (Abu-Musa, 2005).

Nowadays, existing technology solutions are also starting to incorporate interfaces and embedded routines that interact with other solutions, such as security applications that manage configurations and entitlements. This is the first step toward moving organizations closer to continuous monitoring and compliance automation. This capability, however, is still not fully functional for many technology solutions on the market today. Many different types of technology accounting currently exist in the commercial world, e.g. accounting and financial information, communication audits, technical audits, employment accountings, and also more recently, accounting information (Barnier, B; 2009).Cutting *et al.* (1971: 76-77) considers that accountants should: understand and analyze the concentration of controls in an electronic environment; understand accounting information systems and understand the use of computer accounting software. As Accounting Information System (AIS), the accounting related modules of Enterprise Resource Planning (ERP) Systems, ERP have more dominant and complex. Accountants" abilities to audit around the system such as perform their audit without evaluating the reliabilities

accountants' risk assessments and substantive planning decisions. As global institutions seek to link Enterprise Risk Management (ERM), Operational Risk Management (ORM).Information technology risk management continues to expand and gain additional focus within financial services organizations. In addition, executive management is continuing to exert pressure on the information technology risk management function, looking for tangible evidence that it is contributing to the improvement of the business and information technology operations (PricewaterhouseCoopers; 2007). Most organizations are expecting a high return on their investment in information technology risk management.

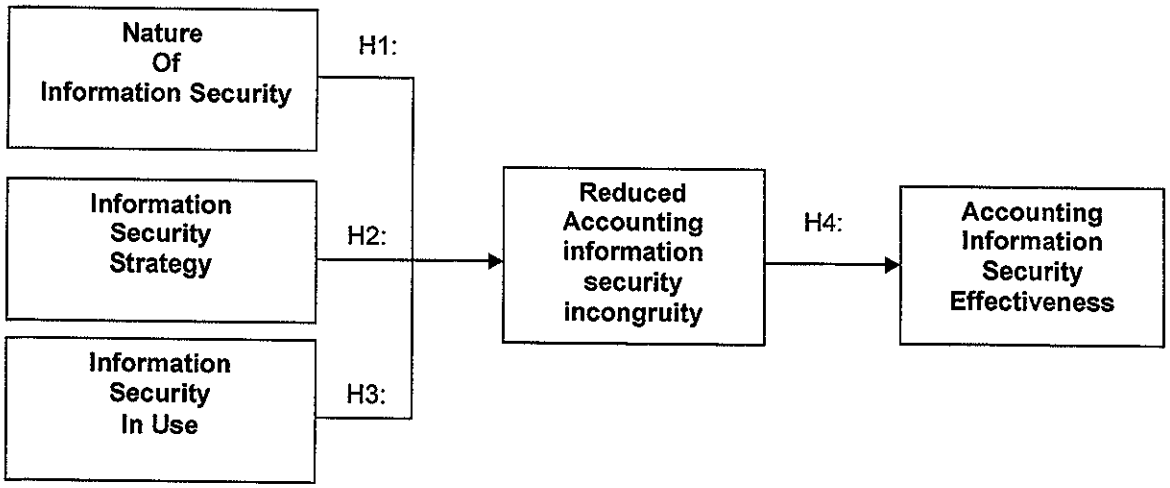
In Thailand, employees' lack of experience in securing accounting information systems mainly due to absence of training on how to protect accounting systems prior to resuming their jobs and lack of effective recruitment processes for accounts executives. There is a lack of knowledge of using technological frames of reference (TFR) to study the accounting information security gap created by incongruent perceptions related to information risk and does not find studies that have examined the relationship between the usefulness of accounting information system and IT Risk in the business sector in Thailand, the benefits of implementing such technologies and identification of the best model for implementation in Thailand to focus their attention on the framework, processes, and drivers of accounting information system security by using technological frames of reference (TFR) to study the accounting information system security gap created by incongruent perceptions related to information risk.

In the next section, the conceptual framework is presented, and a set of testable hypotheses is proposed. Methods of the study are then introduced, which include information about the sample, study measures, data analysis, and test results. Following a discussion of the results, implications and limitations are offered.

2. RELENANT LETERATURE ON ACCOUNTING INFORMATION SECURITY EFFECTIVENES THROUGH TECHNOLOGICAL FRAMES OF REFERNCE

The conceptual model shown in Figure 1 was drawn based on the literature review and uses the responsibilities checklist is intended to assist directors focus is on auditing outcome. TFR is based on work in organizational systems failure and change management by Wanda Orlikowski (W. Orlikowski, 1992, 1993). The framework has been used extensively to investigate the organizational impacts of technology on users.

FIGURE 1 CONCEPTUAL MODEL
ACCOUNTING INFORMATION SYSTEM SECURITY EFFECTIVENESS THROUGH TECHNOLOGICAL FRAMES OF REFERNCE



Accounting Information Systems encompass numerous business applications, such as general ledger, payroll, supply chain management, manufacturing and business intelligence. Although very costly to implement such as ERP systems have been adopted by many companies in recent years due to the potential for lower operating costs, shorter cycle times, and higher customer satisfaction (Brown 1997). Successful adoptions of ERP systems have also been linked to enterprise-wide re-engineering efforts and implementation of best practices (Kumar, K. and J. Van Hillegersberg; 2000). In particular, accounting information systems create substantial concerns about business interruption, system security, database security, and process interdependency risks (Girard and Farmer 1999). As will be discussed, several of these risks may result in greater control risks (e.g., lack of segregation of duties) and/or have a direct, material financial statement impact (e.g., invalid transactions, misclassifications, duplicate payments to vendors, and potential going concern issues relating to business interruptions) or require additional disclosures. Accountants will find it necessary to understand fully the risks associated with new and advanced business information systems, and the controls that are needed to respond to those risks. Companies should put in place effective security programs and associated controls. To ensure continuity, regular penetration tests must be conducted. Such tests might include breaking into access points through persuasion or brute force, or gaining admission as a visitor and trying to access areas for which someone is not authorized. (Caralli, R.; J. Stevens; C. Wallen; D. White; W. Wilson; L. Young; 2007).

1. Technological Frames of Reference: Nature of Information Security, Use of Information Security, Information Security Strategy and Reduced Information Security Incongruity

TFR is based on work in organizational systems failure and change management by Wanda Orlikowski (W. Orlikowski, 1993; W. Orlikowski & Robey, 1991; Yates & Orlikowski, 1992). The framework has been used extensively to investigate the organizational impacts of technology on users. The most often cited and analytically used work in the literature is a study by Orlikowski and Debra Gash which reported on their investigation of how Lotus Notes users' different technological frames of reference led to problems in design, implementation, and use in a large international consulting firm (Wanda Orlikowski & Gash, 1994).

Orlikowski & Gash (1994) argue that the concept of 'technological frames' offers a useful analytic perspective for explaining and anticipating actions and meaning. Technological frames are cognitive structures or mental models that are held and shared by individuals, typically operating in the background with both facilitating and constraining effects. These individual frames of reference are social in nature and have been described as "A built-up repertoire of tacit knowledge that is used to impose structure upon, and impart meaning to, otherwise ambiguous social and situational information to facilitate understanding" (Gioia, 1986, p.56). Orlikowski & Gash (ibid.), researching the introduction of Lotus Notes technology into a consultancy organization, found that three 'domains' characterized interpretations of technology:

Nature of Technology (NoT): People's images of the technology and their understanding of its capabilities and functionality – what technology IS and what it can DO.

Technology in Use (TiU): People's understanding of how the technology will be used on a day-to-day basis – HOW it might be used to create value

Technology Strategy (TS): People understand of why the organization acquired and implemented the technology, its likely OUTCOMES and VALUE to the organization.

Nature of information security implies the procedural, structural, conceptual, or physical reasons for information security implementations or *what* technologies are used for in organizations including capabilities and power of effectiveness (Orlikowski and Gash, 1994). The proper installation and operation (Barnard and von Solms, 2000) of information security artifacts is critical to reducing risk (Dhillon and Backhouse, 2000) and that requires understanding why the artifact was purchased and implemented.

Organizations will understand and use the accounting information system and will intuitively grasp the system. The manager's friend: alerts, warnings, guidance (Siponen, M. T., 2000).

Information security strategy implies *why* organizations implement technologies. The expectations of technology implementation, desired impact supporting organizational goals (Orlikowski and Gash, 1994), strategic partnerships, and goals are critical to business growth and viability and influence risk decisions, even at the member level (Bhagyavati and Hicks, G.,2003).

Businesses see technology as a way of reducing the cost of accounting operations, reduced headcount. Technology seen as a magic bullet, expert system, giving them greater control over non-compliant managers. Believe that Accounting Managers will make managers better at their roles. Believe accounting information system will produce better accounting information (Anderson, J. M., 2003).

Information security in use implies *how* organizations implement technologies such as how workers interact with technology (Orlikowski and Gash, 1994), day to day actual conditions and consequences associated with such interaction (Farahmand, F., Dark, M., Liles, S., and Sorge, B., 2009), or worker views of how the technology is used (Barrett, 1999). This construct may also include process improvements (Davidson, 2002) or overcoming socio-cultural, legal, political, or implementation barriers (Sanford and Bhattacherjee, 2008).

Firms can set the Strategic aspiration often limited to administration and accounting information system services. Accounting Managers desire to make long-term shift in accounting function. Doubt that technology will bring about a shift in strategic focus and Technology is unlikely to impact on professional accounting information system roles (Rotvold, G., et al, (2008).

Reduced Accounting Information Security Incongruity ranges from personal values such as reduced skepticism (Orlikowski and Gash, 1994) to better long-term project planning (Sanford and Bhattacherjee, 2008). RMI is important because when organizational member group views become incongruent with organizational technology use, nature, or strategy, organizations experienced reduced effectiveness (Barrett, 1999), completely derailed projects (Sanford and Bhattacherjee, 2008), or other negative affects (Davidson, 2002; Lin and Cornford, 2000; Shaw, et al., 1997). Reduced member incongruity lends to a more effective organization.

Therefore, posit the hypotheses as below:

H1: *Nature of Information Security is positively associated with the Reduced Accounting Information Security Incongruity*

H2: *Information Security Strategy positively associated with the Reduced Accounting Information Security Incongruity*

H3: *Information Security in Use is positively associated with the Reduced Accounting Information Security Incongruity*

2. Reduced Accounting Information Security Incongruity and Accounting Information Security Effectiveness

Accounting Information Security Effectiveness can range from increased inter-departmental communications (Orlikowski and Gash, 1994) to derived economic benefit (Sanford and Bhattacherjee, 2008). Improved information system effectiveness can also include enhanced user performance (Davidson, 2002), better user perception (Lin and Cornford, 2000), and improved end-user support satisfaction (Shaw, et al., 1997). Reduced information security incongruity leads to improved accounting information security effectiveness. Several studies have attempted to examine the wider impact of IT on overall business performance. While some have been able to identify links between IT strategy and overall firm performance, evidence remains inconclusive. For example, Bharadwaj (2000) and Santhanam & Hartono (2003) found some correlation between companies with high IT capabilities and levels of profitability compared to competitors, while others found evidence that high performing organizations invest a significantly higher proportion of revenues in IT investments than companies with lower performance (Harris & Katz, 1988).Therefore, posit the hypothesis as below:

H4: *Reduced Accounting Information Security Incongruity is positively associated with the Accounting Information Security Effectiveness*

3. RESEARCH METHODS

3.1 Sample Selection

The sample data for this study comprise to 642 CFO of all listed firms in Thailand. The purpose of this survey was to determine user's perceptions of the operational for empirical studies. Deducting the undeliverable from the original 642 mailed, the valid mailing was 14 surveys from which 297 responses were received. Of the surveys completed and returned, only 283 were usable. The effective response rate was approximately 51.56%. According to Aaker, Kumar and Day (2001), the response rate for a mail survey, without an appropriate follow-up procedure, is less than 20%. Thus, the response rate of this study is considered acceptable. Following Armstrong and Overton (1977) tested for differences between early and late respondents and found no significant differences, indicating that non response bias was not a major problem in this study.

3.2 Questionnaire Design and Measurements

3.2.1 Questionnaire Design

The design of the questionnaire of this study is adopted several from sources of data, including previous instruments developed by other researchers and the research framework developed from the relevant literature. Most of the questions were in closed form using a Likert-type scale, all scored on five-point numerical scale from 1=strongly disagree to 5=strongly agree. A half page empty space at the end of the questionnaire is provided to give respondents an opportunity to express anything else that they would like to add. Before using the data collected, the pre-testing was undertaken (Hunt et al., 1982, Presser & Blair, 1994, Babbie, 2005). Pre testing was intended to identify whether there were any ambiguous or unanswerable questions, to identify whether the wording or layout could be adjusted, whether the meaning the researcher believed was associated with a question, and how others perceived it. A draft of the questionnaire was sent to academics at University of Mahasarakham to examine and approve the construct validity. Academics are served as respondents and assist in testing the instrument; comments and suggestions were use to revise the instrument in terms of readability, validity.

3.2.2 Measurements

The design of the questionnaire of this study is newly developed from several sources of data, including previous instruments developed by other researchers and the research framework developed from the relevant literature.

All of the questions are in closed form using a Likert-type scale. All are scored on five-point numerical scale from 1=strongly disagree to 5=strongly agree. The measurement analysis emphasizes explanation of the reliability and validity of new instruments for measuring these constructs.

3.2.2.1 Dependent Variables

Accounting Information System Security Effectiveness measured via 6 items that Cumulative effect of the relationship between information systems experience and the user experience within organizational context.

3.2.2.2 Independent Variables

Reduced Accounting Information Security Incongruity was measured using 6 items to test Realignment of organizational member group perceptions of risk related to information.

Nature of information security measured via 6 items includes Procedural, structural, conceptual, or physical reasons for information security implementations.

Information security strategy was measured using 6 items to test Business requirements governing the design, adoption, and implementation of all security policies, education, and training programs, and technological controls.

Information security in use was measured using 6 items to test Daily interaction with information security artifacts through physical interaction, discussions of use, resulting outcomes conditional on, process improvements based on, and barriers presented by information security artifacts.

3.3 Validity and Reliability

An assessment of the reliability of the constructs and the validity of the instrument were conducted to establish the reliability and validity of the instrument.

Reliability; the most common measure of scale reliability is Cronbach's Alpha. Prior to conducting factor analysis on the data, it was considered useful to check the reliability of the scale used to confirm that the scale used consistently reflects the scale they are measuring (Field, 2005).

Validity; to identify any remaining issues the test instruments pre-testing was undertaken (Hunt et al., 1982, Presser & Blair, 1994, Babbie, 2005). Pre testing was intended to identify whether there were any ambiguous or unanswerable questions, to identify whether the wording or layout could be improved, whether the meaning the researcher believed was associated with a question was how others perceived it.

Factor analysis was firstly utilized to investigate the underlying relationships of a large number of items and to determine whether they can be reduced to a smaller set of factors. The factor analyses conducted were done separately on each set of the items representing a particular scale due to limited observations. With respect to the confirmatory factor analysis, this analysis has a high potential to inflate the component loadings. Thus, a higher rule-of-thumb, a cut-off value of 0.40 was adopted (Nunnally and Berstein, 1994). All factor loadings are greater than the 0.40 cut-off and are statistically significant. The reliability of the measurements was evaluated by Cronbach alpha coefficients. In the scale reliability, Cronbach alpha coefficients are greater than 0.70 (Nunnally and Berstein, 1994). The scales of all measures appear to produce internally consistent results; thus, these measures are deemed appropriate for further analysis because

they express an accepted validity and reliability in this study. Table 1 shows the results for both factor loadings and Cronbach alpha for multiple-item scales used in this study.

TABLE 1
RESULTS OF MEASURE VALIDATION

Items	Factor Loadings	Cronbach Alpha
Accounting Information Security Effectiveness	0.82 – 0.84	0.83
Reduced Accounting Information Security Incongruity	0.84 – 0.86	0.85
Nature of information security	0.82 – 0.84	0.82
Information security strategy	0.81 – 0.85	0.81
Information security in use	0.82 – 0.84	0.82

3.4 Statistic Test

This research uses the Ordinary Least Squares (OLS) regression analysis to test the hypotheses and estimate factors affecting audit performance. Because both dependent and independent variables in this study were neither nominal data nor categorical data, OLS is an appropriate method for examining the hypotheses relationships (Aulakh, Kotabe and Teegen, 2000). In this research, the model of aforementioned relationships is as follows:

Equation 1: $RAISI = ß01 + ß_1NIS + ß_2ISS + ß_3ISU + e$
Equation 2: $AISSE = ß_{02} + ß_4RAISI + e$

Where as:
AISSE = Accounting Information Security Effectiveness; RAISI = Reduced Accounting Information Security Incongruity; NIS = Nature of Information Security; ISS = Information Security Strategy; ISU = Information Security in Use

4. RESULTS AND DISCUSSION

The descriptive statistics and correlation matrix for all variables are shown in Table 2. The results of OLS regression according to hypotheses are estimated as shown in Tables 3.

Table 2 shows the descriptive statistics and correlation matrix for all variables. With respect to potential problems relating to multicollinearity, variance inflation factors (VIF) were used to provide information on the extent to which non-orthogonality among independent variables inflates standard errors. The VIFs range from 1.01 to 2.15, well below the cut-off value of 10 recommended by Neter, Wasserman and Kutner (1985), meaning that the independent variables are not correlated with each other. Therefore, there are no substantial multicollinearity problems encountered in this study.

TABLE 2
DESCRIPTRIVE STATISTICS AND CORELATION MATRIX

Variables	AISSE	RAISI	NIS	ISS	ISU
Mean	3.82	3.76	3. 72	3.84	3.76
AISSE					
RAISI	0.64**				
Nature of Information Security	0.66**	0.56**	0.60**		
Information Security Strategy	0.60**	0.62**	0.58**	0.66**	
Information Security in Use	0.56**	0.61**	0.56**	0.64**	0.62**

* p<.05, ** p<.01

Table 3 presents the results of OLS regression of the relationship between the Accounting Information Security Incongruity on Accounting Information System Security Effectiveness.

The first set of research hypothesis focused on the relationships between the Nature of Information Security; Information Security Strategy; Information Security in Use and Reduced Accounting Information Security Incongruity (Hypotheses 1-3) are shown in Table 3. The evidence indicates that the Nature of Information Security (H1: b_1= 0.62, p < 0.01) has a positive and significant effect on Reduced Accounting Information Security Incongruity. Therefore, Hypothesis 1 is supported.

The Information Security Strategy (H2: b_2= 0.68, p < 0.01) has a positive and significant effect on the Reduced Accounting Information Security Incongruity. Therefore, Hypothesis 2 is supported.

The Information Security in Use (H3: b_3= 0.66, p < 0.01) has a positive and significant effect on the Reduced Accounting Information Security Incongruity. Therefore, Hypothesis 3 is supported.

The second set of the hypotheses concentrated on the relationships between the Reduced Accounting Information Security Incongruity and Accounting Information System Security Effectiveness (Hypothesis 4) in Table 3. The evidence indicates that the Reduced Accounting Information Security Incongruity (H4: b_4= 0.65, p < 0.01) has a positive and significant effect on the Accounting Information Security Effectiveness. Therefore, Hypothesis 4 is supported.

TABLE 3
RESULTS OF OLS REGRESSION ANALYSYS[a]

Independent variables	Dependent Variable	
	RAISI	AISSE
Nature of Information Security	0.62***	
	(0.04)	
Information Security Strategy	0.68***	
	(0.06)	
Information Security in Use	0.66***	
	(0.04)	
RAISI		0.65***
		(0.06)
Adjusted R2	**0.68**	**0.67**

*** p<.01, a Beta coefficients with standard errors in parenthesis.

5. CONTRIBUTIONS

5.1 Theoretical Contributions

The research contributes to the extension of the Technological frames are frames that show how construct meaning from technology and technology-related change. Technological frames are derived from social cognitive theory and were first used in information systems in the seminal article by Orlikowski & Gash. Business knows how can technological frames of reference of other groups be consciously influenced or modified by a different group. Organizations to understand users' capabilities and perspectives with respect to technology and can apply the concept of the technological frame. Organization should be regular reviewing, monitoring and testing of physical, logical and environmental security controls to protect information assets.

5.2 Practical Implications

The results take focus the concept of 'technological frames' offers a useful analytic perspective for explaining and anticipating actions and meaning. Technological frames are cognitive structures or mental models that are held and shared by individuals, typically operating in the background with both facilitating and constraining effects. These individual frames of reference are social in nature and have the tacit knowledge that is used to a consistent process-risk-control framework or model, and focused on improvements in the workflow, efficiencies, and effectiveness of accounting information technology risk management processes. guidance on how to manage IT-related risks, beyond both purely technical control measures and security; Understanding how to capitalize on an investment made in an IT internal control system already in place to manage IT-related risk

6. CONCLUSION

In this study, the model to investigate the IS security frame alignment model that would improve accounting information security effectiveness. The results can used to describe accounting information system security management functions trying to strike a balance between strategic and tactical risk initiatives. Some have addressed their program designs and operating models (roles within the organizational structure, responsibilities, and accountability), the research to examine on using technological frames of reference (TFR) to study the accounting information system security gap created by incongruent perceptions related to information risk. The framework form this research has been used extensively to investigate the organizational impacts of accounting technology on users.TFR is based on work in accounting information s system failure and change management. The framework has been used extensively to investigate the firms' impacts of technology on users. Firms should put in place effective security programs and associated controls.

7. LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

This study emphasizes the importance of the using technological frames of reference (TFR) links accounting information security, but it does not address the issue of how the using technological frames of reference (TFR) should be carried out. This research has some limitations. First, this study emphasizes the importance of the using technological frames of reference (TFR) links accounting information security. Future research could identify the others consequences of the technological frames of reference (TFR). Secondly, used detailed field-based studies, longitudinal case studies, and case surveys and to test different audit environmental influences to each of the factors identified in the model in these difference contexts.

REFERENCE

Abu-Musa, A. Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations, Computer and Information Science, Vol. 18, pp. 1-26, 2005.

Anderson, J. M. (2003). Why we need a new definition of information security. Computers & Security, 22(4), 308-313.

Barnier, B.; 'Driving Value From Nonrevenue-generating Activities: Myths and Misunderstandings of Governance and Risk Management', ISACA Journal, ISACA, USA, 2009

Barnard, L. and von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. Computers & Security, 19(2), 185-194.

Barrett, M. I. (1999). Challenges of EDI adoption for electronic trading in the London Insurance Market. European Journal of Information Systems, 8(1), 1-15.

Bhagyavati and Hicks, G. (2003). A basic security plan for a generic organization. Journal of Computing Sciences in Colleges, 19(1), 248-256.

Craig, J. (1993). Developing a computer use policy at the University of California at Berkeley. Paper presented at the Proceedings of the 21st annual ACM SIGUCCS conference on User services, San Diego, California, United States.

Davidson, E. J. (2002). Technology frames and framing: A socio-cognitive investigation of requirements determination. MIS Quarterly, 26(4), 329-358.

Davidson, E. J. (2006). A technological frames perspective on information technology and organizational change. The Journal of Applied Behavioral Science, 42(1), 23-39.

Dhillon, G. and Backhouse, J. (2000). Information system security management in the new nillennium. Communications of the ACM, 43(7), 125.

Dunkerley, K. and Tejay, G. (2009, August 6th-9th). Developing an Information Systems Security Success Model for eGovernment Context. Paper presented at the Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, CA.

Farahmand, F., Atallah, M., and Konsynski, B. (2008). Incentives and perceptions of information security risks. Paper presented at the Twenty Ninth International Conference on Information Systems, Paris, France.

Farahmand, F., Dark, M., Liles, S., and Sorge, B. (2009). Risk perceptions of information security: A measurement study. Paper presented at the 2009 International Conference on Computational Science and Engineering, Vancouver, Canada.

Farahmand, F., Navathe, S. B., Enslow, P. H., and Sharp, G. P. (2003). Managing vulnerabilities of information systems to security incidents. Paper presented at the Proceedings of the 5th international conference on Electronic commerce, Pittsburgh, Pennsylvania.

PricewaterhouseCoopers with IIA, 'IT Risk—Closing the Gap: Giving the Board What It Needs to Understand, Manage and Challenge IT Risk', USA, 2007

Orlikowski, W. J. and Gash, D. C. (1994). Technological frames: making sense of information technology in organization

Rotvold, G. (2008). How to create a security culture in your organization. Information Management Journal, 42(6), 32-34, 36-38.

Sanford, C. and Bhattacherjee, A. (2008). IT implementation in a developing country municipality: A sociocognitive analysis. International Journal of Technology and Human Interaction, 4(3), 68-93.

Vaast, E. (2007). Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. The Journal of Strategic Information Systems, 16(2), 130-152.

AUTHOR PROFILE:

Dr.Aukkaradej Chaveerug earned his Ph.d. at Mahasarakham Business School, Mahasarakham University, Thailand in 2009. Currently he is a Lecturer of Accounting Major at the Mahasarakham Business Scholl, Mahasarakham University, Thailand.

อัตราแลกเปลี่ยนสกุลเงินต่างประเทศ
วันที่ 20 พฤษภาคม 2557

	USD	AUD	GBP	CAD	CNY	EUR	HKD	INR	IDR	JPY	THB
US$	1	1.079	0.594	1.088	6.238	0.7307	7.752	58.69	11475	101.32	32.5
Australia	0.927	1	0.551	1.008	5.78	0.677	7.183	54.382	10632.74	93.883	30.115
Britain	1.683	1.816	1	1.831	10.496	1.23	13.044	98.758	19308.98	170.491	54.688
Canada	0.919	0.992	0.546	1	5.732	0.671	7.123	53.928	10543.97	93.099	29.863
China	0.16	0.173	0.095	0.174	1	0.117	1.243	9.409	1839.62	16.243	5.21
Euro Zone	1.3686	1.477	0.813	1.489	8.537	1	10.609	80.323	15704.69	138.667	44.48
Hong Kong	0.129	0.139	0.077	0.14	0.805	0.094	1	7.571	1480.282	13.07	4.193
India	0.017	0.0184	0.0101	0.0185	0.1063	0.0124	0.1321	1	195.5188	1.7264	0.5538
Indonesia	0.0001	0.0001	0.0001	0.0001	0.0005	0.0001	0.0007	0.0051	1	0.0088	0.0028
Japan	0.01	0.011	0.006	0.011	0.062	0.007	0.077	0.579	113.255	1	0.321
New Zealand	0.859	0.927	0.51	0.934	5.355	0.627	6.655	50.385	9851.288	86.983	27.901
S.Korea	0.001	0.0011	0.0006	0.0011	0.0061	0.0007	0.0076	0.0573	11.1951	0.0988	0.0317
Malaysia	0.311	0.335	0.185	0.338	1.938	0.227	2.409	18.238	3565.879	31.485	10.099
Philippines	0.023	0.025	0.014	0.025	0.143	0.017	0.177	1.342	262.346	2.316	0.743
Singapore	0.798	0.862	0.474	0.869	4.98	0.583	6.189	46.858	9161.677	80.894	25.948
Taiwan	0.033	0.036	0.02	0.036	0.207	0.024	0.257	1.946	380.559	3.36	1.078
Thailand	0.031	0.033	0.018	0.033	0.192	0.022	0.239	1.806	353.077	3.118	1