Conference Book

THE 2nd ICBB and CSR-UN CONFERENCE

- International Conference on Business and Banking
- Corporate Social Responsibilty University Network Conference

Kuta - Bali, 2-3 Februari 2012

Supported by:

UNIVERSITI SAINS MALAYSIA

Universitas Warmadewa

PERBANAS INDONESIAN BANKS ASSOCIATION

IBI Ikatan Bankir Indonesia

Telkom Indonesia

bank sinarmas

BANK MASPION

BANK Syariah BUKOPIN

BANK YUDHA BHAKTI
Memahami dan Memberikan Yang Terbaik

CONFERENCE PROGRAM

The 2nd International Conference on Business and Banking
&
Corporate Social Responsibility University Network Conference

Inna Kuta Beach Bali Hotel Indonesia, 2 – 3 February 2012
Jl. Pantai Kuta No. 1 - Kuta, Bali - Indonesia

Dates	Time (Bali Time)	Program
Wednesday February 1, 2012	13.00 – 18.30	Registration
Thursday February 2, 2012	08.00 – 08.05	Opening Soni Harsono (Chair Committee)
	08.05 – 08.15	Welcome Speech + Opening Ceremony Prof. Dr. Tatik Suryani (Rector of STIE Perbanas Surabaya)
	08.15 – 08.25	Welcome Speech Prof. Dato' See Ching Mey (Deputy Vice – Chancellor (ICM) - USM)
	08.25 – 08.35	MOA Signing
	08.35 – 09.15	Keynote Speech 1 Keynote Speech 2
	09.15 – 09.30	Photo Session
	09.30 – 09.45	Coffee Break
	09.45 – 12.15	Parallel Session 1 (3 rooms)
	12.15 – 13.15	Lunch
	13.15 – 15.45	Parallel Session 2 (3 rooms)
	15.45 – 16.00	Coffee Break
	16.00 – 18.30	Parallel Session 3 (3 rooms)
	17.40 – 18.30	CSR Panel Discussions (Room Pasamuan 2) "CSR in Malaysia: Strategies for Engaging Community, Business and University"
	19.00 – 21.00	Dinner and Cultural Evening
Friday February 3, 2012	09.00 – 16.00	City Tour (optional)

Dinner & Cultural Night

Dates	Time (Bali Time)	Program
Thursday February 2, 2012	19.00 – 19.15	Closing Ceremony (Dance from Warmadewa University)
	19.15 – 19.25	Closing Speech (Vice Rector STIE Perbanas Surabaya Dra. Lindiawati, MM)
	19.25 – 19.35	Closing Speech (Rector Warmadewa University Prof.Dr. I Made Sukarse
	19.35 – 19.45	Best Paper Anouncement (Nurul H. U. Dewi, M.Si) Best Paper 1 : Prof. Wilopo Best Peper 2 : Prof.Dr.I. Made Sukarse Best Paper 3 : USM
	19.45 – 19.50	Photo Session
	19.50 – 20.05	Cultural performance (dance)
	20.05 – 20.20	Participant testimony (3 persons)
	20.20 – 21.00	Dinner
	21.00 – 21.05	Closing = MC

THE THREAT LEVEL TOLERANCE IN THE COMPANY OF ACCOUNTING INFORMATION SYSTEM[1]

Dian Indri Purnamasari
Universitas Pembangunan Nasional "Veteran" - Yogyakarta
Email: indri_mtc@yahoo.com

ABSTRACT

Accounting information system developments that provide benefits in many organizations it has risks that are not light. How can an organization tolerate the possibility of a threat in accounting information system will be different with other organizations. This study wante know whether there are differences in levels of tolerance to the threat of companies in accounting information system. With a sample of all companies listing on the Indonesia S Exchange (IDX) and the rate of return of 18.8% of respondents, this study provides a statis conclusion that there is no difference in the level of tolerance to the threat of accoun information system among companies listing on the IDX. This is because companies are lis on the IDX is a company that is ready for the public so that they also prepare all the th associated with information systems, including accounting information system and the maxin fine.

Key words: *Accounting, System, Information, Threat, Tolerance*

INTRODUCTION

Information system has advanced rapidly with the development of computer-based technol In the field of accounting, the development has resulted in Accounting Information Syst (AIS). Today, it is hardly possible for companies (organizations) not to adopt computerized A There are a lot of things to do with the computerized AIS, among others, organizing increasingly globalized activity at the international as well as local level. Activities in m organizations were made easier with the presence of computerized AIS. For exam organizations were no longer need to perform data transmission via postal service that ta much longer time, but over the internet protocol. In fact, it is possible for them to excha information on accounting data with the help of computers and the Internet.

Development of the AIS, which provides many benefits and advantages to organizati brings also no small risk, which is a threat contained in the input, process, or output. A mistake in accounting data entry, whether committed intentionally or not, can have signifi impact on the operating activities of the organization, and this is one of the threats to the syst Accounting data loss due to a defect in storage system and to the error in AIS design might a jeopardize organizational activities. Any development of AIS has positive and negative effe and it is no secret to many organizations that develop and use the system. The question subsequently arises is how much effort an organization should expend on anticipating the thre Although much has been done by accountants in designing AIS to reduce the threat in it,

[1] This research funded by the Directorate General of Higher Education, Ministry of National Education, Researcl Lecturer in the program Youth and Women's Studies, 2007

nd for the use of this system continues to increase (Musa, 2001). How much effort ıded to anticipate the threat is reflected in the organizational tolerance for the possible ts in the AIS.

How one organization tolerates the possible threat in the AIS can be different to that of er. Perhaps, some organizations are so strict in designing AIS that they will not tolerate any t or, in other words, they will directly address the emerging threats, so it is not possible for to reappear. In contrast, some other organizations might still tolerate such a threat so it is ble that the same threats will appear several times within a certain period of time.

Musa (2004) in his study, which used a sample of all organizations in Saudi Arabia, uded that there was no significant difference between the various organizations in that ry in terms of tolerance for threats to the computerized AIS. Some types of threats are often ienced by many companies, which indicate a similar degree of tolerance for the threat in Among these threats are the mistakes made by employees in entering data, and it is very ıble because it is humane. The author in this study intends to determine whether the ıizations in Indonesia have the same tolerance level for threat in the AIS.

Based on the background of the research mentioned above, the problem formulation will there any differences in the degree of tolerance to the threats in AIS among companies at IDX? The current study aims to provide empirical evidence of whether there are ences in the level of tolerance to the threats in among all companies enlisted at IDX. It is uthor's hope that this research will be beneficial to the development of AIS, especially for ıanies that went public, in tolerating threats in AIS.

ERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

l according to Hollander (1980 in Sihwahjoeni and Gudono 2000) is the processes of tion, grouping, and interpreting. Forgus and Melamed (1976 in Desriani 1993) stated that is the information extraction process. In Encyclopedia of Psychology it is described that shows the sensory experience in the form of information about people, objects, and events, ell as psychological processes to refine the information. Kamus Besar Bahasa Indonesia 5) defines level as direct response (acceptance) to something or a process through which an idual knows something through his/her senses. Rakhmat (1993 in Eko 2001) defines that represents an experience about objects, events, or relationships acquired by inferring mation and interpreting messages. Level is a process by which a person interprets stimuli e has received and also a process by which a person organizes his or her thoughts by ıreting or experiencing them, and by processing the signs or anything happens around ıet. Thus, level can be interpreted as cognitive processes experienced by every person in standing any information about environment through the five senses (Sihwahjoeni and ıno 2000).

However, because the level of objects or events depends on a framework of space and time ard, 1985 in Eko 2001), it will also be very subjective and situational in nature. In addition

to being implicitly stated in the definition above, this argument is also consistent with proposed by Rakhmat (1993 in Eko 2001) that level is determined by personal and situati factors, which Krech and Crutchfield (1997 in Eko 2001) referred to as functional and struc factors. The functional factors are derived from needs, past experiences, and other th included in what is referred to as personal factors. Therefore, what determines the level is no type or form of stimuli, but the characteristics of person who respond to them. Structural fac derived solely from the physical and neurological effects they cause on the nervous syster individuals. Therefore, according to Kohler and Wartheimer (1959 in Eko 2001), basec Gestalt theory, if we intend to improve something then we improve it as a whole. To p differently, if we want to understand an event we can not examine the facts separately, bu must look at the overall relationship.

Tolerance is how events or threats to AIS may occur within a certain period. If the thr to AIS are frequently occurred, then the tolerance is so high that they were allowed to o repeatedly. If the company does not tolerate the threats to AIS, it will handle them as emerged and anticipated to prevent them from happening in the future. AIS designs were n to realize an effective and efficient system of internal control, which, among others, is directe put off the threat to SIA within the organization.

Loch et. al. (1992) conducted a test at the managerial level of the Managen Information Systems (MIS) to determine the security level of the microcomputer, mainfr computer and network environment. In their research, Loch et. al. (1992) developed the th level to the MIS into 12 levels, and respondents were asked to rank the highest threat (top ra Respondents in the study stated that the threat of natural disasters (e.g. the threat of hackers ineffective control) and errors by employees are the two things ranked at the top of t selection.

Davis (1996) replicates the study by Loch et. al. (1992) with the respondents that v members of the Information Systems Audit and Control Association (ISACA) and Certi Public Accountants (AICPA). He concluded that auditors with different AIS computeri environment will have different levels of tolerance of threats to AIS. Computerized syst associated with parties outside the company will have a higher risk level than a system tha only related to the environment within the company.

Ryan and Bardoloi's (1997) study categorized threats to AIS into 15 instruments, distributing questionnaires to information systems technicians of medium and large compa that are organizing a conference. The results showed that different companies have diffe tolerance levels against threats to AIS, although the threat in the form of errors by the emplo still occupying the highest ranking of each respondent. Instrument in this study still has m shortcomings, according to some opinions of other investigators, and thereby need to modified and refined in the future.

ISBN : 978 – 602 – 99879 – 1 - 1

Henry (1997) attempted to identify to what extent the companies provide the level of erance to AIS threats which is reflected by the level of security in entering the system. The dy concluded that 80% of companies have already backed up their information systems, 75% ve been securing their system by creating a password, while the rest just do security to address possibility of computer viruses. This shows that in fact many companies have different erance levels against threats to AIS.

Musa (2001) classifies the threats to AIS into 19 instruments and applies them to the nking companies in Egypt. Instrument developed in this study adopted and perfected that of evious research mentioned above and using 5-point scale on the frequency of threat in the mpanies. The results showed that there was no difference in levels of tolerance to the AIS eats among the types of different banks.

Musa (2004) developed his previous study using a sample of all organizations in Saudi abia. He concluded that there was no significant difference between different organizations in udi Arabia in terms of tolerance to the threats that occur in computerized AIS. Some types of eats that are often experienced by many companies indicate a similar tolerance to the threat of AIS, such as the employee made mistakes in entering the data, which is a very tolerable and mane.

This study replicated that of Musa (2004) because, as far as the author concerned, similar idies have not been conducted in Indonesia by using a sample of all ISX-listed companies. fferent types of companies will have different tolerance levels against threats in the AIS, for ample: Banks will have a lower tolerance level compared to other types of companies as banks other financial institutions have a greater risk in terms of their customer finance than real tate companies.

Based on the above findings, the author formulated the following hypothesis:

There are differences in the level of tolerance to AIS threats among IDX-listed companies.

ESEARCH METHOD

etermination of Sample

ıe sample in this study is the population of all IDX-listed companies. The selected respondents ere the companies' internal auditors because they are able to design the AIS and to detect any eaknesses in it. The choice of companies enlisted at IDX is because they are public companies at require greater control in terms of AIS and should not tolerate any threat in it. A question to answered in this study is whether in fact this is so. The data was collected through mail rveys.

lentification and Measurement of Variables

olerance for threat to AIS was measured using instruments developed by Musa (2004) which mprised 19 items of question about the possible frequency of the occurrence of the threat in

AIS. Respondents were asked to answer how often the threat is happening within the compa a 5-point scale (had never, almost never, sometimes, often and always).

Validity and Reliability Testing

The research data will not be useful if the instrument used to collect them do not hav reliability and validity (Cooper and Schindler, 2001). Reliability testing is intended to dete the extent to which the measurement is consistent. An instrument is reliable if it has a Cro alpha greater than 0.6 (Hair et.al., 1998). Validity testing was to evaluate how well the meas instrument measures what it is supposed to measure. A variable is valid if it has factor lo larger than 0.4 and eigenvalue greater than 1 (Hair et.al., 1998).

Pilot Test

Before the questionnaire is given to the actual respondents, the author conducted a pilot t determine the validity and reliability of the instrument and to avoid questions that are obvious as well as to determine the time required to complete the questionnaire. The pilo was conducted with 30 respondents who work as internal auditor in company and the r showed that all the research instruments used are valid and reliable.

Nonresponse Bias Test

The test of nonresponse bias was conducted to investigate whether there was a significant different in the characteristics of the sample of the respondents who responded and did not respond. They were divided in to two, which are the respondents who came early and represented those responding and the respondents who came late and represented those not responding and then t-test was conducted.

Hypothesis Test

The hypothesis test was conducted using *One Way ANOVA.*

DATA ANALYSIS AND DISCUSSION

Data Description

The following table illustrates the process of distributing questionnaires to obtain data and rate of return.

Total questionnaire distributed	= 339
Returned and analyzed	= 64
questionnaires	=
Response rate	18,8%

Table 1: Questionnaire Response Rate

Total of 339 questionnaires were distributed to internal auditors in IDX-listed companies, an number returned for analysis amount to 64 questionnaires. The response rate is quite

ıse in general the response rate in Indonesia is in the range of 10%, whereas in the study it ıed 18.8%.

Company	Amount
Farming and Fishing	3
Mining	2
Manufacture	33
Transportation	4
Telecomunication	2
Retails	6
Banking and Financial Service	10
Others	4
Total	64

Table 2. Data on Companies Returning Questionnaire

above table shows that the companies returning questionnaire are mostly of manufacture ;) and banking (15%). This was so because the composition of manufacturing and banking ɔanies enlisted at IDX outnumbered other type of companies, i.e. 43% and 30% for ıfacturing companies and banking and financial non-banking companies, respectively.

response Bias Test

results showed that there was not any significant difference in the respondents who did not ɔnd or submit them. Therefore, there was not any problem of response bias.

dity and Reliability Testing

result of validity and reliability testing show that all of accounting information system ble are reliable with 19 questioners and the cronbach alpha 0,910 and valid use pearson lation analysis.

riptive Statistics

riptive statistics this research is:

Variable	N	Minimum	Maximum	Average	Estándar Deviation
SIA	64	2,95	4,84	3,96	0,49

Table 3. Descriptive Statistics

mining Anova Assumptions

ɔthesis testing using the ANOVA requires several assumptions tests that must be met in r that the results of ANOVA can be used to make a conclusion about this study. Anova ɪnptions to be fulfilled are (Ghozali, 2005):

a. *Homogeneity of variance*
Dependent variable in this study should have the same variance in each categor independent variables. Levene test results used to see the homogeneity of variance w significance level > 0.05 concluded that the group has the same variant or, in other w the assumption of equal variance was met.

b. *Random sampling*
For the purpose of significance testing using ANOVA, sampling within each group taken randomly and the sample taken in this study is the entire population. Anova re robust even if the sampling was not random, and subsequent analysis can be performed.

c. *Multivariate normality*
The variables must be normally distributed, but Anova remain robust even if it was normally distributed, and subsequent analysis can be performed. The variables in this s were normally distributed so that the normality assumption fulfilled.

Assumption of ANOVA test showed that all assumptions are met so that the hypothesis te using ANOVA can be continued in subsequent analysis.

Hypothesis Testing

Variabel	Uji F	Signifikansi
SIA	1,657	0,139

Table 4. Hypothesis Testing

The table shows the statistical significance of 0.05, which means there is no difference in level of tolerance for the threat of AIS among the companies enlisted in IDX. Test results s that H_a is not supported. It is not supported because the IDX-listed companies were ready fo public so that they also prepare all the things related to the information systems, including and in maximum effort. Reasonably good and tightly enforced regulation and supervision f the various parties associated with the procedures and processes even when they were pu companies (e.g. Bapepam) has contributed a great deal to make these companies a concerned about the development of company information systems. This has made t companies minimize the risk or threat in the AIS, and they no longer give a lot of toler against possible threats in the AIS, such as providing passwords to other parties by the emplo They already have a good control system for AIS, so there is no difference in the leve tolerance for threat in AIS among IDX listed companies, or in other words they have the s tolerance level for threat to AIS because they realize the importance of security in informa systems, including AIS.

Company	Amount	Average
Farming and Fishing	3	4,43
Mining	2	4,39
Manufacture	33	4,09
Transportation	4	3,98
Telecomunication	2	3,81
Retails	6	3,73
Banking and Financial Service	10	3,69
Others	4	3,34
Significance		0,054

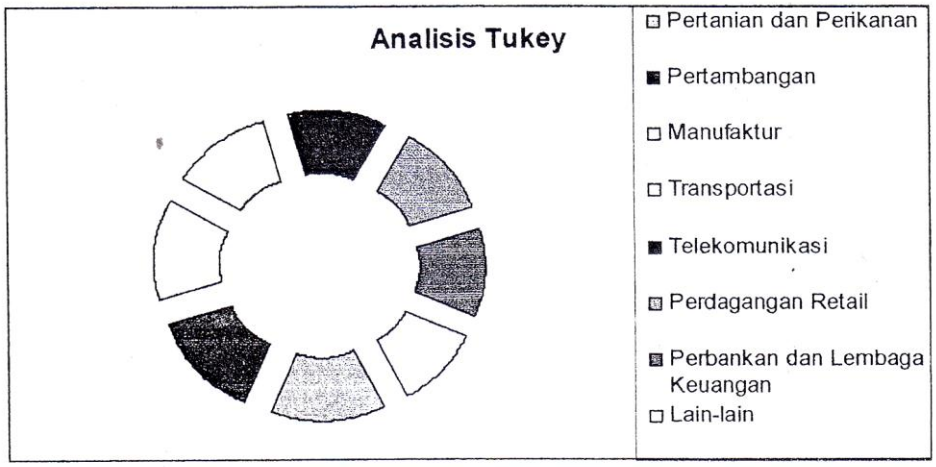

Table 5. Tukey Analysis

e table above shows the average value of the tolerance level of each type of companies for the S threat. Significance level of 0.054 showed that the average level of tolerance of each type of mpanies for AIS thrats did not differ statistically with a significance level of 5%. The results pport the decision that there was no difference in the level of tolerance for AIS threat among X-listed companies.

CONCLUSION, IMPLICATION, SUGGESTIONS, AND LIMITATIONS

Conclusion

This study concluded that among 18.8% IDX-listed companies there are statistically difference in the level of tolerance for threat to AIS. This is because they are the companies are ready for the public so that they also prepare all the things related to information syst including AIS with both maximum and reasonably good effort. The companies enlisted in have gone through several stages of the process of fulfilling the requirements made under supervision of many external parties in IDX so they have the same rules for IDX lis Similarity of the rules and procedures makes the levels of safety and tolerance for threats in has no difference between them.

Research Contribution

The results of this study contribute to the development of AIS in the form of finding that f with a lot of supervision in the form of regulation from various parties appeared to have the s AIS development, especially their perception of threat to AIS. It certainly would disting them from other companies that have no regulation or supervision from various external parti

Limitation and Suggestion

This study has limitation in its sample, i.e. the companies enlisted in IDX with less moderate response rate of 18.8%. This gives a great opportunity for future research to expanc study population to all companies in Indonesia and compares the various possible type structure of corporate ownership.

REFERENCES

Boynton, Wiiliam C., Raymond N. Johnson dan Walter G. Kell, 2003, *Modern Auditing*, John Wiley & Sons

Cooper, Donald dan Pamela S. Schindler, 2001, *Business Research Methods*, 7th edition, McC Hill, Singapore

Davis, Charles E, 1996, *Perceived Security Threats to Today's Accounting Information Syst A Survey of CISAs*, IS Audit & Control Journal, Vol. 3, pp. 38-41

Desriani, Rahmi, *Tingkat Akuntan Publik Terhadap Kode Etik Akuntan Indonesia*, Thesis Program Pasca Sarjana, Universitas Gajah Mada, 1993.

Eko Prasetyo, Januar, *Tingkat Perusahaan Asing Dan Perusahaan Dalam Negeri Yang Tidak Public Terhadap Kebutuhan Jasa Akuntan Publik*, JAAI Volume 5 No. 1, Juni 2001.

Hair, Joseph, Rolph Anderson, Ronald Tatham dan William Black, 1998, *Multivariate I Analysis*, 5th edition, Prentice Hall International Inc, New Jersey

Henry, Laurie, 1997, *A Study of The Nature and Security of Accounting Information Syst The Case of Hampton Roads, Virginia*, The Mid-Atlantic Journal of Business, Vol. 33, 63, pp. 171-189

Loch, Karen D., Houston H. Carr and Merril E. Warkentin, 1992, *Threats to Informa Systems: Today's Reality, Yesterday's Understanding*, MIS Quarterly, June, pp. 173-186

Musa, Abu, Ahmad A., 2001, *Evaluation The Security of Computerized Accounting Informatic Systems: An Empirical Study on Egyptian Banking Industry,* PhD. Thesis, Aberde University, UK

_____, 2004, *Exploring The Perceived Threats of Computerized Accounti Information Systems in Emerging Countries: An Empirical Study on Saudi Organizatio* The 7th European Conference on Accounting Information Systems, 30th-31st March 200 Prague, Czech Republic

Ryan, S.D. and B. Bordoloi, 1997, *Evaluating Security Threats in Mainframe and Client/Serv Environmets,* Information & Management, Vol. 32, Iss. 3, pp. 137-142

Sihwahjoeni, M. Gudono, *Tingkat Akuntan Terhadap Kode Etik Akuntan*, Jurnal Riset Akuntar Indonesia, Volume 3, No. 2, Juli 2000.