International Journal of Communication & Information Technology (CommIT) http://msi.binus.ac.id/commit/
Vol. 8 No. 2 October 2014, pp. 44-54

MEASUREMENT OF APPLICATION OF ISO 27001 OF CUSTOMER CELLULAR CARD CONFIDENTIALITY DATA IN PT. XYZ AREA JAKARTA

Krishna Rahadian[1]; Ahmad Juang Pratama[2];
[1]Information Technology Service Quality Measurement, Astra Graphia Information Technology
Jakarta, Indonesia, kentan9_9oyenk@yahoo.com
[2]Industrial Engineering Department, Faculty of Science and Technology, Al Azhar Indonesia University
Kompleks Madjid Agung Al Azhar, Jakarta 12110, Indonesia

Abstract: The purpose of this study was to evaluate the effects of the process of ISO 27001 with respect to the confidentiality of customer cellular card Jakarta and to improve cellular card customer data confidentiality at PT.XYZ from data leakage of the customer data due to the third party involvement, clean-desk policy, and access right. Recommendation regarding the improvement is provided after reviewing the confidentiality of customer data. The survey in this study is conducted by questionnaire. From the evaluation results of the questionnaire, it is concluded that the larger customer data leaks are mainly caused by the external factors.

Keywords: ISO 27001; Confidentiality; Test Validity; Questionnaire; External Factors

INTRODUCTION

Security and confidentiality problem is one important aspect of data or information. This thing is very related to how important those messages, data and information, which are sent and received by party or person of interest.

When someone accesses information, there is a relation between Access Control and Human Resource Security with Confidentiality. Human Security has to focus on its individuals. Access Control is one of the keys of service security in information and system safety [1–2]. Access control and human resource security are included in 11 ISO 27001 domain and in inside there is indicators of ISO 27001 procedure like third party policy, clean desk policy, access right. ISO 27001 is an international standard for information security that has aspects of information security in a company [3–10].

It is expected that by analyzing this customers' confidentiality data, customers' trust to that company increases more and the company gains more customers [11–17]. Thus, writer will discuss about customers' confidentiality data whether application of ISO 27001 in PT. XYZ has included all information security factors to customers' cellular card data in Jakarta?

The problems discussed in this work are: how is the result of implementation of ISO 27001 in PT. XYZ especially related to third party policy, clean desk policy, and access right? What are the factors that cause of leakage of customers' data in PT. XYZ? How are the ways to prevent leakage of customers' data related to customers' cellular card confidentiality data in PT. XYZ?

The goals in this work are: (i) to evaluate implementation process of ISO 27001 to customers' cellular card confidentiality data at PT XYZ; (ii) to recommend revision of customers' cellular card confidentiality data in PT. XYZ especially related to third party policy, clean desk policy, and access right, and (iii) to increase customers' cellular card confidentially data in PT. XYZ.

METHOD

The basics of ISO 27001 implementation is PDCA process. The Plan-Do-Check-Act (PDCA) is industry standard of managing the continuation of business function [3]. The PDCA model is applied to identify the company management needs. The PDCA supports the review and revision of the management needs.

The number of samples required by this research was determined by the Slovin formula of the following,

$$n = \frac{N}{1 + Ne^2},$$

where n is the sample size, N is the population size, and e is the error tolerance.

The metric or parameter or measure of qualitative study is used for measurement or comparison or tool to track performance of a process. From business side, the metric is measurement which is used to measure some qualitative components like

performance of a process, organization or investment (ROI). With this metric, then the data were collected, analyzed to provide information for a organization in setting their next business strategy to achieve the goals.

Goal of metric for security management is to manage efficiency of all activities of information security. SLA, contract and policy security are needed to manage and control management security process.

In this research, to change data from qualitative and quantitative, the researchers use Likert scale.

The validity testing is obtained by correlating each indicator score with the total of indicator score, then the result of correlation is compared with critical value at significance level 0.05.

The *R* value that is obtained from each item or r_{count} will be compared with r_{table} value for $\alpha = 0.10$. If $r_{count} > r_{table}$, then that item is considered as valid; otherwise, the item is not valid and is not used.

In this research, the reliability calculation uses Alpha formula Arikunto of:

$$\Gamma 11 = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum \sigma b^2}{\sigma t^2}\right)$$

The primary data were collected through survey and interview.

Primary data are: company profile, organization structure, data about ISO 27001 application toward customers' confidentiality data in PT. XYZ and also interview with related IT security and business continuity division.

Secondary data are obtained from questionnaire, books, e-books, articles and journals.

A number of types of analysis was performend in this work: (i) general analysis of PT. XYZ; (ii) the current business process conditions such as business process and organization structure especially in IT security and business continuity division; (iii) the analysis of the application of ISO 27001 to customers' confidentiality data; and (iv) the analysis of the application of ISO 27001 mainly to customers' confidentiality data about how the result of output is to customers' cellular card of PT. XYZ after application of ISO 27001.

RESULTS AND DISCUSSION

Before the implementation of ISO 27001 in PT. XYZ all employees' activities or vendors haven't fulfilled security standard. Based on result of writer's observation and evaluation of IT security division in PT. XYZ there are several factors that affect customers' confidentially data of PT. XYZ like third party policy, clean desk policy and access right for application, network and database.

Writer's reason of doing review of these three indicators like third party policy, clean desk policy and access right is because this is more related with the secrecy of customers' data and these three indicators are very clear about the difference of before and after the implementation of ISO 27001 (IT security). For review that is done from third party policy, clean desk policy and access right, it can be seen clearer in Table 1.

In PT. XYZ, the more developing the technology is, the more human resource is needed, one of the things that is done by PT. XYZ is with cooperation with third party in work process. At first it is only in accordance with agreement between two parties and SLA (Service Level Agreement), work process that is signed by third party. Here are some of disadvantages of third party policy: there is not any NDA signing for each third party employees, all employees in PT. XYZ vendor have not been recorded, and there is not ID-card to differentiate between third party employees and employees in PT. XYZ.

Based on observation that is done by IT security division in PT. XYZ, before implementation of ISO 27001, almost all employees in PT. XYZ do not notice confidentiality data which are personal data they have. These evidences were found in the company: Messy desk with important documents; In each discussion use whiteboard with discussion result that is not erased afterward; if a flash disk is not at table, it is still plugged in laptop or CPU; sometimes laptop or computer doesn't use password; lack of employees' consciousness about confidentiality; and at printer, sometimes there are documents that is not thrown away or destroyed immediately if it isn't used anymore.

In PT. XYZ user account to login application or network or database still uses PT. XYZ employees' user account so it cannot be differentiated between the users when they access. This condition is susceptible to cause customers' data leakage so customers' confidentiality data in PT. XYZ is included in not stiff category.

Here are some drawbacks of access control: for application access, network and database still uses user-ID of employees in PT. XYZ; third party employees hasn't been recorded and made their own user-ID after signing NDA; and there is not reset password of user-ID periodically.

Before the implementation of ISO 27001, there are targets that are wanted to be achieved. Whether it is for customer of for continuity of PT. XYZ business. If a telecommunication company has already had ISO 27001, it is additional value for customers' trust in using PT. XYZ cellular card and certainly with more public moves to use PT. YXZ cellular card will affect continuity of PT. XYZ business, revenue in PT. XYZ will increase more and also will increase the PT. XYZ

Table 1: Review Confidentiality (procedure checklist)

Review Confidentiality	Procedure	Before ISO 27001	After ISO 27001
Third party policy	NDA signing	Available	Available
	there is all third party employees	Not yet	Have noted all and detail
	Special ID-card of third party	Not yet	Available
Clean Desk Policy	Messy desk with important documents	Available	Available
	Whiteboard with discussion result that is not erased	Available	Erased
	Flash disc sometimes is plugged in laptop or CPU n	Available	No
	Sometimes using laptop or computer without using password	Available	All use Password
	Lack of consciousness of confidentiality in employees	Available	No
	At printer, sometimes there are documents that is not thrown away or destroyed immediately if it isn't used anymore	Available	No, already neat
Access right	For access, network and database application still use PT. XYZ employees' user-ID	Available	No, but depend on the need
	Third party employees haven't been recorded and made their own user-ID after signing NDA	Available	No, but depend on the need
	There isn't reset password of user-ID periodically	Hasn't been periodically yet	Already periodically

cellular card customers.

From the company side, several targets that wanted to be achieved after the implementation of ISO 27001 are: (a) Guarantee the continuity of PT. XYZ business; (b) If the continuity of PT. XYZ goes smoothly, then it will increase revenue in PT. XYZ; (c) Decrease interference of PT. XYZ business operation by preventing and decreasing the effect of happened security incident; (d) Prevent leakage of important data in PT. XYZ because many daily operational in PT. XYZ are related to third party; (e) Additional value if it is compared with the competitors.

Meanwhile, from the customer side, those targets are: (a) Increase customers' trust; (b) Increase amount of PT. YXZ customers; and (c) Customers will feel safer towards the secrecy of their data.

From all domains and metric procedures of ISO 27001, for the result of the calculation can be seen in Table 2.

In the second audit, the process of auditing takes 10 sampling servers or personals and there is also some additional factors for the calculation. In this second audit, it is expected that the targets that are wanted to be achieved can get successful result. For the result, it can be seen in Table 2.

After the result of calculation of metrics ISO 27001 on January-February, there is several factors which do not achieve the targets from the expected result. It is expected by often doing evaluation in each audit and by recommending revision to management in PT. XYZ to achieve the targets.

Some factors that have not yet achieved the targets: still not all third party uses ID-card in PT. XYZ work place; still not all third party signs NDA; and all employees in PT. XYZ haven't totally done clean desk policy

Access for application that is used by third party, sometimes 1 user-ID can be used for several people. There is increase in calculation of metrics on June which can be seen on the table below:

From evaluation of twice audit of ISO 27001, there are some factors that are increased but not from all domains ISO 27001 because even though there is a domain that doesn't achieve increase or 100% result can't be said as not successful, but it must be seen from the situation and condition when the calculation of metrics. To see the comparison of twice audit of ISO 27001 it can be seen in Fig. 1.

From Fig. 1, it can be seen that there are some ISO domain that increase but there are also some decrease. But seeing from the result, it can be concluded that ISO 27001 process of PT. XYZ increases and continues to undergo evaluation for revision.

The goal of doing third party policy is to make rules for third party access of asset information, third party responsibility, and asset security information of PT. XYZ.

Evaluation of third party policy is done after calculating metrics above, as following: (i) Each access information of PT. XYZ from third party has to known by related employees in PT. XYZ; (ii) Each third party employee who accesses sensitive information has to sign NDA that is for information security data of PT. XYZ; and (iii) Each third party employee has to understand information security procedure and policy of PT. XYZ.

The goals of clean desk policy are to build employees' security and trust culture in PT. XYZ, to increase security and confidentiality data, to reduce risk and threat from unauthorized access that causes data leakage, and to increase neat work place,

Evaluations for clean desk policy are: all flash disks, laptops, portable hard disks must be stored in locked drawer, whiteboard must be cleaned or erased after discussion, and after work hour done, all documents must be put in order and stored in locked drawer.

The aim to make sure who access application, network and database of PT. XYZ is right person. From the result of calculation of metrics ISO 27001, there are several evaluations like: register User-ID of third party from service center to ID creation, to reset password, it is done based on user data, to access application, network, and database of PT.XYZ user-ID must be below User-ID owner's responsibility,

and to make user-ID data become secret.

There are several steps which become writer's recommendation for next revision, here are the steps: First, useful socialization and training in revision process in implementing ISO 27001. As for all procedure process and policies must have been approved by management. Socialization can be done by several ways as following: (a) Training or seminar about ISO 27001. (b) Direct simulation in PT. XYZ work place. (c) Using brochure, banner that are placed in place where it is easy to be seen by all employees that is to increase care about information security. (d) Through e-mail, internal magazine, or other media communication.

Second, apply policies that are related with application of ISO 27001 strategy that aims for balancing an activity that is being run in PT. XYZ. For example, if it is doing a project activity with third party, each process will be noted in log or form filling that supports policy and procedure in revision. As for processes that supports this policy and procedures are: (a) Requirement for application security (requirement for minimum password, time-out session, authentic, and others). (b) Non Disclosure Agreement (agreement to maintain secrecy) for third party. (c) License and standard software that are used

Third, measurement of control effectiveness intends to achieve information security target. Control which has been set either policy, procedure or standard that are measured about the effectiveness by studying results of application that is noted or written in report or relevant forms. Measurement method has to be set before, then the control effectiveness is measured periodically in accordance with the needs. For example: (a) Access right closure: all access rights which undergo mutation/ stop working have to be closed maximum 2 days after the status is reported officially to management. This measurement can be done once in 6 months. (b) All third parties (vendor, consultant) that enter data center must be accompanied by employees of PT. XYZ. (c) All sensitive computer equipments have applied strong password. (d) All PT. XYZ employees in work unit that is put in scope must have followed socialization/training about information security.

Table 2: Result of Metrics Quartal-1 2012 calculation in PT. XYZ

ISO27001 Control	ISMS (Policy, Procedure/standard)	Metrics	Measuring Mechanism
Organization of information security	Third Party Access Policy	82% of Third party personnel using badge	Spot checking , sampling on 5 vendor in city plaza
		82% of Third party personnel signing NDA	Spot checking , sampling on 5 vendor in city plaza
		82% of Third party personnel accessing internal network via VPN/APN	Spot checking , sampling on 5 vendor in city plaza
Asset Management	Information Classification and Handling Procedure	45% employee stating document classification on their day to day document	Interview IT personnel (sampling 7 IT personnel)
Human Resource Security	Security training and awareness Policy	50% Number of newsletter published	Checking number of news letter publish
	Teleworking procedure	50% Valid remote access and application user	Request access report from IT Datacommops and IT custodian
Physical and environmental security	IT Data Center management procedure	98% of visitor accessing data center with SPK	Request report from IT Data center
Communication and operations management	Virus handling policy	55% of virus that automaticity cleaned by anti virus 55% of employee desktop/ notebook not by passing anti virus	Request report from IT OSO Spot checking, sampling on 7 IT Personnel
	Removable media policy	55% Employee not storing PT.XYZ sensitive data in their flashdisk	Spot checking, interview Sampling 7 IT personnel
	Network Access Policy	55% Availability of network access log, remote access log	Discussion with IT Datacomm personnel
	Capacity planning	55% Availability of sizing analysis document for each server	Sampling 10 server and discuss with IT Infrastructure Development. Checking if they have sizing analysis document (capacity analysis).
Access control	Password policy	60% Strong credential on server	Sampling 3 server and 3 hash for each server. Brute force their hash
	Clean desk policy	60% employee comply to clean desk policy	Enforcement clean desk activity (weekly activity)
Information security incident management	Information security incident response procedure	100% Availability of information security incident review activity	Security incident document report
Business continuity management	Disaster recovery plan	20% matching application version between DR and production	Interview IT Custodian (EAI, Single Mediation, SPR, Cookies, MKIOS, Payment gateway)
		20% Match data (database) between DR & production based on time	Request backup restore report from IT DDR
Communication and operation management	Capacity planning	55% Availability of sizing analysis document for each server	Sampling 10 server and discuss with IT Infrastructure Development. Checking if they have sizing analysis document (capacity analysis).

Table 3: Result of Metrics Quartal-2 2012 calculation in PT.XYZ

ISO27001 Control	ISMS (Policy, Procedure/standard)	Metrics	Measuring Mechanism
Access control	Information Access Restriction	90% of applications implementing access control list	Sampling 10 application
	User password management	90% Strong credential on server	Sampling 10 server/application/database. Brute force their hash
	Information Access Restriction	90% of database instances implementing access control list	Sampling 10 database instance
	Clear desk and clear screen policy	90% employee comply to clean desk policy	Enforcement clean desk activity
	Information Access Restriction	90% of server implementing access control list	Sampling 10 server
Asset Management	Inventory of asset	40% of valid asset inventory (infrastructure)	Sampling 10 server /device. Compare with assets in CMDB
Business continuity management	Testing, maintaining and assessing business continuity plan	58% matching application version between DR and production	Interview IT Custodian
		58% Match data (database) between DR & production based on time	interview/ request documents
Communication and operations management	Monitoring system use	100% SIEM correlation rule review has been done	Discussion (OSSC, SIEM Custodian, IT SSC)
	Network controls	100% Legal WAP	Spot checking IT working environment (City Plaza)
	Information back-up	100% testing restore have been done	Checking restore testing document
	Controls against malicious code	100% of employee desktop / notebook has updated antivirus	Spot checking. Sampling 10 IT Personnel
	Audit logging	100% Availability application log	Interview, sampling 10 application log
	Monitoring and review of third party service	100% of third party SLA achieved	Sampling 10 third party SLAs
	Controls against malicious code	100% of virus that automatically cleaned by anti virus	Checking log of virus cleaned by another anti virus
Compliance	Intellectual property rights	60% employee not installing unlicensed software	Interview / Spot checking/Report from Information System Management
Human resource security	Removal of access rights	100% Valid application / system user	Request access report from Application custodian
	Information security awareness, education and training	100% Number of security newsletter published	Checking number of news letter publish
Information security incident management	Reporting information security events	100% Availability of information security incident review activity	Security incident document report
Information system acquisition, development and maintenance	Technical vulnerability management	60 % of penetration test finding has been remediated	Review penetration test report
	Security requirements analysis and specification	60% of CR release with security impact that through security testing. Including application which never been security-tested	Checking release calendar
	Security requirements analysis and specification	60% CR Process document complete	Interview, documents checking, Application testing. Sampling 10 applications
Organization of information security	Addressing security in third party agreements	100% of Third party personnel accessing internal network via VPN/APN	Sampling. Spot checking on 10 vendor in city plaza
	Addressing security in third party agreements	100% of Third party personnel signing NDA	Sampling. Spot checking on 10 vendor in city plaza
Physical and environmental security	Physical Entry controls	100% of Third party personnel using badge	Sampling. Spot checking on 10 vendor in city plaza

Table 4: Metrics calculation on June 2012 in PT. XYZ

ISO27001 Control	ISMS (Policy, Procedure/standard)	Metrics Jan-Feb 2012	Metrics June 2012
Organization of information security	Third Party Access Policy	82% of Third party personnel using badge	100% of Third party personnel using badge
		82% of Third party personnel signing NDA	100% of Third party personnel signing NDA
		82% of Third party personnel accessing internal network via VPN/APN	100% of Third party personnel accessing internal network via VPN/APN
		60% Strong credential on server	90% Strong credential on server
		60% employee comply to clean desk policy	90% employee comply to clean desk policy
Access control	Password policy	60% Strong credential on server	90% Strong credential on server
	Clean desk policy	60% employee comply to clean desk policy	90% employee comply to clean desk policy

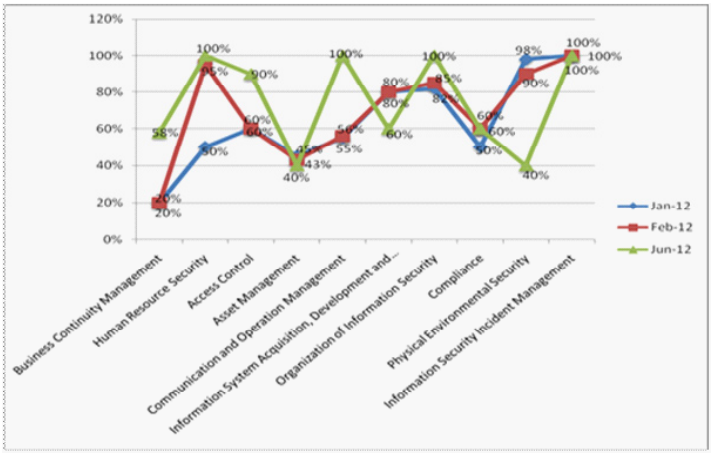

Fig 1: graphic of metrics of ISO 27001 on Jan-Feb and June

Fourth, doing internal audit to guarantee that the application of ISO 27001 is done precisely in accordance with set of policy and procedure. Internal audit must be done by employee/team that has competence in auditing ISO. Employee/team that does internal audit must be set by management and leader who have authority through official decision letter and assignment letter.

Fifth, doing review to perfecting implementation of ISO 27001 by revising all policies, procedures or standards that have been set then the effectiveness is evaluated. Then checking which policy and procedure that have been set correctly and haven't. If procedure hasn't been set precisely, do an analysis why that thing happens. Whether it is because of short time of socialization or it is because of too hard or unpractical procedure. The result of control effectiveness measurement and report about internal audit are also evaluated to check which control that hasn't achieved the target, still weak (ineffective) or that still becomes finding in internal audit. All control weaknesses has to be revised immediately or perfected so it doesn't cause the same weakness/ mistake later.

For the conclusion of the observation result and analysis for information clarification, it concludes that: (i) Confidentiality: Asset information is very sensitive and has high risk about access leakage and misusing that can disturb smoothness of institution/ agency business temporally or disturb image and reputation of the company. Examples: customers' cellular card data of PT. XYZ, IP address, computer password, audit report; (ii) Internal: Information that has been distributed widely in internal surrounding of PT.XYZ which the spread internally doesn't need permission of the owner of information and the risk of unauthorized spread don't cause any significance loss. Examples: PT. XYZ policy, work manual, work procedure, work instruction, training material and information that are provide in internet; and Public/ external: Information that is coincidentally provided by institution/agency can be known by public.

In this thesis research, there will be four variables investigated for questionnaire that will be

spread, the variables are: (i) Internal factor: This variable will give picture from internal factor side how the effect of ISO 27001 towards customers' confidentiality data. Customers will give valuation that is being felt right now after the implementation of ISO 27001. The indicators for internal factors are: Customers secrecy data: Seeing from customers' opinion about secrecy of customers' data, whether according to them it is fitted with ISO 27001 (IT security); and Customers security data: this is customers' valuation about customers' data security, whether it is fitted with international standard. (ii) External factor: External factor variable gives pictures of factors that affect customers' data leakage out of company scope. Customer will give valuation about customers' confidentially data leakage of PT. XYZ that is caused by external factor. Below, it is indicator of external factor variable: Customers' data leakage: This is customers' valuation about data leakage that is caused by external factors. Customers' trust: This variable gives pictures about customers' trust towards the implementation of ISO 27001 that affects customers' confidentiality data of PT. XYZ. Below, this is the indicator of customers' trust variable: Customers' trust: To see whether after ISO 27001, customers more believe PT. XYZ or there are other factors that make customers not believe Pt. XYZ. (iii) Customers' confidentiality data: This variable is safe since it is owned by customers towards confidentiality data of PT. XYZ customers. This is the indicators of customers' confidentiality data variable: ISO 27001 (IT Security):

To see how far ISO 27001 (IT Security) affects customers secrecy data.

This questionnaire consists of 20 statements that represent four variables that are examined. These four research variables in form of that questionnaire are variables about internal factor, external factor, customers' trust, and customers' confidentiality data.

Questionnaire about internal factor variable consists of 3 statements, external factor variable consists of 5 statements, customers' trust variable consists of 6 statements and customers' confidentiality data variable consist of 6 statements.

Based on questionnaire and Likert scale, then each questionnaire in internal factor variable has 15 as the highest value and 3 as the lowest value, in external factor variable 25 is the highest value and 5 is the lowest, in customers' trust variable has 30 as the highest value and 6 as the lowest, and in customers' confidentiality data variable has 30 as the highest value and 6 as the lowest.

From the result of Slovin formula calculation with the population of 80 respondents and 10% of error tolerance is got the result of 45. In conclusion writer will spread about 45 questionnaires. These 80 respondents are total of employees that work handling complaint directly about customers of cellular card of PT. XYZ through outlets or second layer (BES). These employees in work process are included in internal of PT. XYZ but in work status they are included in external, so it can be said as internal/external. Because this questionnaire data is not directly from customers of cellular card of PT. XYZ, then this questionnaire is secondary data.

After getting amount of questionnaire sample that is wanted by writer, before questionnaire is whole spread, writer does validity and reliability testing before about 30 answers of respondents' questionnaire.

In table r, for df = amount of case, or for this case df = 30 and 10% significance level, there are 0.296 point where the result of r of each item (variable) can be seen in Corrected Item – Total Correlation column. If the result of r is positive, and r result > r table, then item or that variable is valid.

In this initial stage writer tries to spread 30 questionnaires and tests the validity, after trying calculate using SPSS there are 1 indicator which is not valid in customers' trust variable in question number 7. The results are shown in Table 5.

For internal factor variable from 30 respondents to test the validity, its 3 indicators are valid. It is because r result is bigger than r table value (0.361). So, for internal factor variable, all indicators can be used to spread questionnaire to other respondents.

In external factor variable, the result of calculation using SPSS for all indicators gets result of r value is bigger than r table, so for all indicators of external factor variable are stated as valid.

Customers' trust variable from 7 questions which the validity is tested by writer, there is one question that result of r is smaller that r table. It is the seventh question. Result of r value that is got from SPSS calculation is 0.011 while the minimum of limit of error is 10% from tested validity from 30 respondents, the result of r value has to be bigger than r table value which is 0.296. So for question number seven, it is not valid. Thus, for next questionnaire spread, this seventh question must be deleted.

For confidentiality variable, the result of customers' data calculation using SPSS for six indicators gets result of r value is bigger than r table value. So for all indicators, they are valid.

Next, reliability testing will be done to see how far the measurement tool can be relied and trusted. Reliability is measure that shows used measurement tool in research has reliability as measurement tool, including measured through the consistency of measurement result time from time if the tested phenomena do not change.

Table 5: Internal factor of cellular card of PT. XYZ

No.	Indicator	R Table (10%)	Corrected Item-Total Correlation	Result
	Customers secrecy data:			
1	Customers cellular card secrecy data of PT. XYZ is safer with ISO 27001 (It security)	0.296	0.601	Valid
2	Customers secrecy cellular card access database has fitted ISO 27001 (IT security)	0.296	0.413	Valid
	Customers security data			
3	Customers' security cellular card data of PT. XYZ has fitted ISO 27001 (IT security)	0.296	0,575	Valid

Table 6: External factor of cellular card of PT. XYZ

No.	Indicator	R Table (10%)	Corrected Item-Total Correlation	Result
	Customers data leakage:			
1	Credit card making, or registration in which fills personal data is one factor of external data leakage	0.296	0,442	Valid
2	The other way to do broadcast text is by randomizing numbers	0.296	0,480	Valid
3	The other way to do broadcast text is by randomizing numbers	0.296	0.400	Valid
4	There is person who leaks customers secrecy cellular card data of PT. XYZ	0.296	0.379	Valid
5	Customers often get call from unknown number	0.296	0.657	Valid

Table 7: Customers' trust in cellular card of PT. XYZ

No.	Indicator	R Table (10%)	Corrected Item-Total Correlation	Result
	Customers' trust :			
1	Customers of cellular card of Pt. XYZ aren't affected by cheap fare war	0.296	0.500	Valid
2	With ISO 27001 (IT Security) it increases customers' trust level toward customers cellular card confidentiality data of PT. XYZ	0.296	0.460	Valid
3	Customers trust cellular card of PT. XYZ because of its security quality	0.296	0.531	Valid
4	Customers more believe in company that has already had ISO 27001 (IT Security)	0.296	0.651	Valid
5	Customers cellular card secrecy data is better than the competitors	0.296	0.378	Valid
6	Cellular card data leakage of PT. XYZ isn't caused by lack of security in PT. XYZ	0.296	0.494	Valid

Table 8: Customers confidentiality data

No.	Indicator	R Table (10%)	Corrected Item-Total Correlation	Result
	ISO 27001 (IT Security) :			
1	Minimizing customers cellular card data leakage of PT. XYZ	0.296	0.741	Valid
2	Access for customers secrecy data of cellular card of PT. XYZ is tighter	0.296	0.599	Valid
3	Guarantee the security of customers cellular card data of PT. XYZ	0.296	0.562	Valid
4	Text broadcast is more affected by external factor	0.296	0.562	Valid
5	Text broadcast received by customers is less	0.296	0.720	Valid
6	Customers feel safer with the secrecy data	0.296	0.530	Valid

Reliability testing is related to consistency, accuracy and predictability of a measurement tool. The result of reliability testing in each variable in this research can be seen in Tables 9–12.

Table 9: Reliability of internal factor

Reliability Statistics	
Cronbach's Alpha	N of Items
,767	4

Table 10: Reliability of External factor

Reliability Statistics	
Cronbach's Alpha	N of Items
,729	6

Table 11: Reliability of Customers' trust

Reliability Statistics	
Cronbach's Alpha	N of Items
,752	6

Table 12: Reliability of customers confidentiality data

Reliability Statistics	
Cronbach's Alpha	N of Items
,771	7

Based on tables above, it is seen that all cronbach alpha values range from 0 to 1, as a result internal factor, external factor, customers' trust, and customers' confidentiality data variable can be concluded as reliable.

Conclusion of Questionnaire

Internal Factor

The result of internal factor questionnaire is there are 25 respondents who agree with first question and 2 respondents strongly agree. For doubtful, there are 14 respondents and 4 respondents who disagree. For first question it can be concluded that more than 50% respondents agree that customer secrecy data of cellular card of PT. XYZ is safer with available ISO 27001 (IT security).

For second question there are 4 respondents answer doubtful. But there are more than 50% respondents who agree with second question with 30 respondents and 11 respondents strongly agree with access of secrecy of customers' cellular card database of PT. XYZ has fitted ISO 27001 (IT security).

In third question, there are 24 respondents who agree and 4 respondents who strongly agree. But there are 2 respondents who disagree and 15 respondents state doubtful. With more than 50% respondents agree with third question, it is concluded that security of customers' data of PT. XYZ has fitted ISO 27001 (IT security).

External factor

The first question in external factor questionnaire has 21 respondents who agree and 8 respondents who strongly agree with this question. Along, there are 2 respondents who disagree and 14 respondents state doubtful. It is seen from the result that it is more than 50%, it means respondents agree that credit card making or registration that fill personal data is one of the external factors that causes data leakage.

The second question gets 22 respondents who agree and 7 respondents strongly agree with second question and only 15 respondents state doubtful along with 1 respondent that disagrees. With the value of more than 50% respondents that agree with this question that people trade cell number that they own.

For the other way to do broadcast text is by randomizing numbers question, there are 28 respondents agree and 9 respondents strongly agree but there are 3 respondents that disagree and 5 respondents choose doubtful. With the value of more than 50%, it can be concluded that respondents agree with this third question.

The fourth question has 23 respondents who agree and 9 respondents who strongly agree with this question. In addition, there are 3 respondents that disagree and 5 respondents state doubtful. But with the value of more than 50% respondents that agree with question of there are people who leak secrecy of customers' cellular card data of PT. XYZ.

The fifth or the last question from external factor which is about customers often get call from unknown number has 25 respondents who agree and 10 respondents who strongly agree, 8 respondents are doubtful, and 2 respondents who disagree. It is seen from value that more than 50% respondents agree, it means respondents agree with this question.

Customers' trust

In question about Customers of cellular card of PT. XYZ aren't affected by cheap fare war gets 25 respondents who agree and 4 respondents who strongly agree. In addition, there are 16 respondents that are doubtful. From the value of more than 50%, respondents agree that customers' trust aren't affected by cheap fare war.

With 28 respondents agree, 3 respondents strongly agree and 14 respondents state doubtful in the second question about customers' trust, then it can be concluded that with value of more than 50%, customers believe that with ISO 27001 (IT security) increase customers' trust towards their secrecy data in PT. XYZ.

The third question gets 25 respondents who agree and 5 respondents who strongly agree with the question about customers trust cellular card of PT. XYZ because of its safety, even though there are 14 respondents that state doubtful and 1 respondent disagrees. But the ones that agree are more than 50%.

For the fourth question, there are 24 respondents agree and 13 respondents strongly agree, and 8 respondents state doubtful. It is concluded that with the value of more than 50%, respondents agree with customers more trust company that has already has ISO 27001 (IT security) question.

23 respondents agree and 3 respondents strongly agree with the question about customers cellular card secrecy data of PT. XYZ is better than the competitors with the result of more than 50% respondents agree although there are 18 respondents that are doubtful and 1 respondent disagrees.

In the sixth question, there are 25 respondents who agree and 6 respondents who strongly agree that customers data leakage isn't caused by lack of information security in PT. XYZ. And there are 13 respondents who are doubtful and 1 respondent disagrees.

Customer confidentiality data

In the first question, there are 27 respondents agree and 9 respondents strongly agree, 1 respondent disagrees and 8 respondents are doubtful. With the result of more than 50%, it can be concluded that with ISO 27001 (IT security) customers believe it can minimize customer cellular card data leakage of PT. XYZ.

24 respondents agree and 13 respondents strongly agree, along with 7 respondents who are doubtful and 1 respondent disagrees with the second question. With the value of more than 50%, it can be concluded that Access for customer secrecy data of cellular card of PT. XYZ is tighter.

In the third question, there are 24 respondents agree, 13 respondents strongly agree, and 8 respondents are doubtful. The question about Guarantee the security of customer cellular card data gets result more than 50%.

For question about text broadcast is more affected by external factor is agreed by 20 respondents, strongly agreed by 9 respondents, and is doubted by 16 respondents. From the result of more than 50%, respondents agree with this question.

By getting 20 respondents agree, 15 respondents strongly agree, the question about text broadcast received by customers is less, they are agreed by respondents, although there are 8 respondents who are doubtful, 1 respondent disagrees and 1 respondent strongly disagree.

In the fifth question which is about customers feel safer with the secrecy data, it has 21 respondents agree, 12 respondents strongly agree and 11 respondents are doubtful, along with 1 respondent disagree. With the result of more than 50%, then it can be concluded that respondents agree with this question.

From all results of 45 respondents questionnaire, all variables get result more than half of respondents or more than 50% agree with the questions. So it can be concluded that customer data leakage is not from internal factor of PT. XYZ but from external factor of PT. XYZ. While for customers' trust level, customers more believe with PT. XYZ although competitors have cheaper fare. Customers more believe PT. XYZ since they opine that after ISO 27001 (IT security), customer confidentiality data is felt safer.

CONCLUSION

At the end of this study, conclusion of implementation of ISO 27001 in PT. XYZ for third party policy is that each third party employees' detail logging has to be noted and it is compulsory to sign NDA. Other than that, each third party employees must also follow rules that are in PT. XYZ work place. For clean desk policy, employees of PT. XYZ should obeyed procedure based on ISO 27001. PT. XYZ employees' desks have been neat and no more flash disk that is plugged in computer laptop when that employee leaves his desk. Procedure for registration and erasing access right are revised for customer confidentiality data and to minimize customer data leakage.

Factors that affect customer data leakage are external factors because customer data leakage is caused by irresponsible people by randomizing cell number to offer good or service and also to do crime. For example, fraud text that asks customers to transfer money or fill credit in swindler's number. ISO 27001 hasn't reached external factor.

To protect customer security of confidentiality data and to minimize customer data leakage, PT. XYZ does information security according to international standard which is by implementing ISO 27001. After implementation of ISO 27001, PT. XYZ still does review and revise for next audit process continuously.

REFERENCES

[1] E. Newman, "Critical human security studies," *Review of International Studies*, vol. 36, pp. 77-94, 2010.

[2] M. Masood, A. Ghafoor, A. Mathur , "Conformance Testing of Temporal Role-Based Access Control Systems," *IEEE Transactions on Dependable and Secure Computing*, v. 7, pp. 144-158, 2010.

[3] S. T. Arnason, K. D. Willet, *How to Achieve 27001 Certification*, New York. Auerbach Publication, 2008.

[4] A. Aczel, J. Sounderpandian, *Complete Business Statistics*, New York: McGraw-Hill Higher Education, 2009, retrieved from http://highered.mcgraw-hill.com/sites/dl/free/0073373605/582605/Chapter16_SamplingMethods.pdf

[5] A. M. Fal', "Standardization in information security management," *Cybernetics and Systems Analysis*, vol. 46, pp. 512-515, 2010.

[6] S. A. Ajiboye, "Measuring Process Effectiveness Using Cpm/Pert," *International Journal of Business and Management*, vol. 6, pp. 286-295, 2011.

[7] J. Brenner, "Iso 27001: Risk Management And Compliance," *Risk Management*, vol. 54, pp. 24, 2007.

[8] J. Crampton, H. Khambhammettu, "Delegation in role-based access control," *International Journal of Information Security*, vol. 7, pp. 123-136, 2008.

[9] J. Drtil, "Impact of information security incident theory and reality," *Journal of Systems Integration*, vol. 1, pp. 44-52, 2013, retrieved from http://www.si-journal.org/index.php/JSI/article/viewFile/144/112

[10] F. Farahmand, S. B. Navathe, G. P. Sharp, P. H. Enslow, "A Management Perspective on Risk of Security Threats to Information Systems," *Information Technology and Management*, vol. 6, pp. 203-225, 2005.

[11] Z. Jourdan, R. K. Rainer, T. E. Marshall, F. N. Ford, "An Investigation Of Organizational Information Security Risk Analysis," *Journal of Service Science*, vol. 3, pp. 33-42, 2010.

[12] B. Khoo, P. Harris, S. Hartman, "Information Security Governance Of Enterprise Information Systems: An Approach To Legislative Compliant," *International Journal of Management and Information Systems*, vol. 14, pp. 49-55, 2010.

[13] E. Lomas, "Information governance: information security and access within a UK context," *Records Management Journal*, vol. 20, pp. 182-198, 2010.

[14] E. Rednic, "IT Solution for Security Management in the Cadastral Field," *Informatica Economica*, vol. 15, pp. 160-166, 2011.

[15] C. Teddlie, and F. Yu, "Mixed Methods Sampling: A Typology With Examples," *Journal of Mixed Methods Research* , vol. 1, pp. 77-100, 2007, retrieved from http://www.sagepub.com/foundations/includes/jmmr_journal.pdf

[16] J. M. Unam, "Materials Management For Business Success: The Case of the Nigerian Bottling Company Plc," *International Journal of Economics and Management Sciences*. vol. 1, pp. 50-56, 2012, retrieved from http://www.managementjournals.org/ijems/7/IJEMSi12i1705.pdf

[17] K. Zhou, M, Lv, G. Wang, B. Ren, "Control for Manufacturing Process in Networked Manufacturing Environment," *Journal of Service Science and Management*, vol. 2, pp. 107-116, 2009.