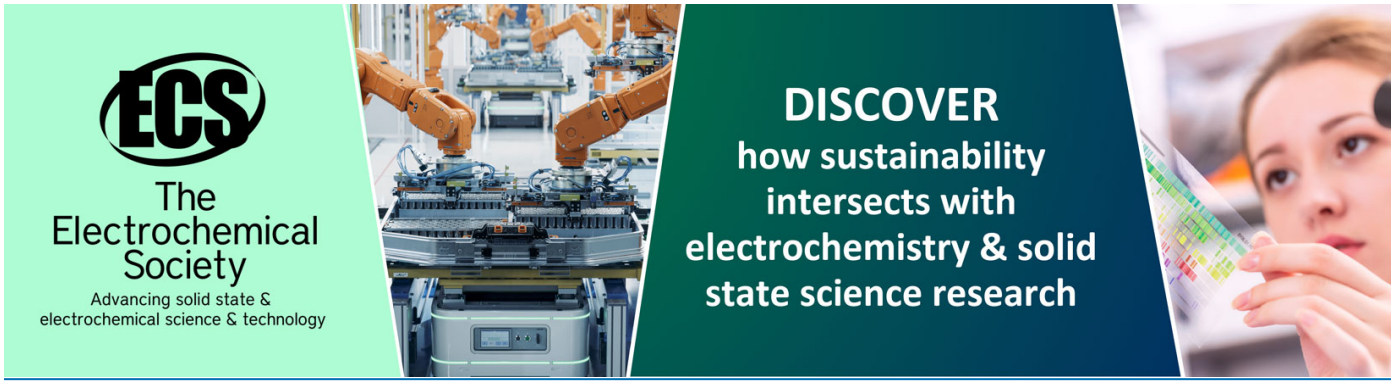
Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet



Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet

Ahmad Nurul Fajar[1], Hendy Christian [2], Abba Suganda Girsang[3]
[1] Information Systems Management Department, BINUS Graduate Program-Master of Information Systems Management, Bina Nusantara University Jakarta, Indonesia 11480
E-mail : afajar@binus.edu
[2] Information Systems Management Department, BINUS Graduate Program-Master of Information Systems Management, Bina Nusantara University Jakarta, Indonesia 11480
E-mail : hendy.christian@binus.org
[3] Computer Science Department, BINUS Graduate Program-Master of Computer Science, Bina Nusantara University Jakarta, Indonesia 11480,
Email : agirsang@binus.edu

Abstract. Every organization must ensure that information assets are protected and information security system has been implemented well. PT. IndoDev Niaga Internet is a provider of business solutions applications and implementation services that include application Human Resource Information System (HRIS) and Enterprise Resource Planning (ERP). In order to ensure the security of the information, then in 2015 PT. IndoDev Niaga Internet implement ISO 27001: 2013. Through the implementation of ISO 27001: 2013, it is expected that information can be properly maintained, which in turn will affect the business continuity. Companies need to know the extent to which the process has been applied and what actions can be done to improve the performance of the application of ISO 27001: 2013. Factor analysis was conducted first to determine the factors that affect to the information security. After the factors that affect to the information security known, then observation and interview conducted to gather data about PT. IndoDev Niaga Internet ISO 27001:2013 implementation according to the factors that affect. And then recommendation and corrective action developed using gap analysis method. The most influential factor to the security of customer information PT. IndoDev Niaga Internet is a factor access control and security operations. For the audit results ISO27001: 2013 from the aspect of access control, they found 11 check items that fit into the category of NC (Non-Conformance) of 33 check items in which 9 of them in the category of major and two remaining categories minor, while for operations security aspects of the 12 check items, found 5 that goes into the category of NC (Non-Conformance) and everything was included into the category of minor.

1. Introduction

Currently, businesses relied and depended on the information to operate the business daily operations to achieve the goals and objectives of the organization [1]. In this digital age, it has become common for organizations to use information systems to process information within the organization in order to get a better support to the achievement of the organization's mission [2].

Thus, every organization must ensure that information assets are protected and information security system has been implemented well [3]. PT. IndoDev Niaga Internet is a provider of business solutions applications and implementation services that include application Human Resource Information System (HRIS) and Enterprise Resource Planning (ERP). PT. Indodev Niaga Internet has handled more than 500 customers spread across the country and abroad. In order to ensure the security of the information, then in 2015 PT. IndoDev Niaga Internet implement ISO 27001: 2013. Through the implementation of ISO 27001: 2013, it is expected that information can be properly maintained, which in turn will affect the business continuity PT. IndoDev Niaga Internet. But over the implementation of ISO 27001: 2013, companies need to know the extent to which the process has been applied and what actions can be done to improve the performance of the application of ISO 27001: 2013. Empirical data in this place shown the trigger to concern about information security management implementation. Therefore, the research undertaken will discuss the evaluation of the application of ISO 27001: 2013 in PT. IndoDev Niaga Internet.

2. Literature Study

The purposes of information security is to protect organization resources, such as, information, hardware, and software [4]. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [5].Three main concepts in information security are confidentiality, integrity, and availability (CIA) [6]The purpose of security management information is information confidentiality, integrity, and availability [3].Information security management system is needed because of the threat to the confidentiality, availability, and integrity of information that organizations large and likely to increase [7].The process of information security management is defined as the cycle of PDCA (Plan-Do-Check-Act), in which management identifies the process that should be implemented, to investigate whether all the processes that have been implemented have been investigated and operations that take into account the feedback and results [3]. ISO 27001: 2013 provides specifications for information security management systems along with practice [7].ISO 27001 also adopted a process model PDCA (Plan-Do-Check-Act) [8]. ISO 27001: 2013 has 14 security control clauses that contain a total of 35 control objectives and 114 controls [9]. The 14 security control clauses as following: Information security policies, Organization of information security, Human resource security, Asset management, Access control, Cryptography, Physical and environmental security, Operations security, Communications security, System acquisition, development, and maintenance, Supplier relationships, Information security incident management, Information security aspects of business continuity management, Compliance. The indicators used in this study refers to the implementation guidance on the control of the ISO 27001: 2013 are set out in the code of practice for information security controls from ISO 27002: 2013. The indicators can be seen in Appendix A.

3. Research Method

Factor analysis was conducted first to determine the factors that affect to the PT. IndoDev Niaga Internet information security. The questionnaire used for gathering the data that will be used in factor analysis. Questionnaire developed using information security indicator that found from literature study. The scale used in this study is the Likert scale (1-5). Likert scale is intended to find out how to agree and disagree respondents to the statements in the questionnaire. After the factors that affect to the PT. IndoDev Niaga Internet information security known, then observation and interview conducted to gather data about PT. IndoDev Niaga Internet ISO 27001:2013 implementation according to the factors that affect.

And then recommendation and corrective action developed using gap analysis method according to the target that has been established by PT. IndoDev Niaga Internet and the current achievement of that target. Literature study also used to develop recommendation and corrective action.

4. Results and Analysis

This research was conducted at PT. IndoDev Niaga Internet by distributing questionnaires to 119 employees in IT-related departments. Reliability analysis to test the validity and reliability of the questionnaire study was conducted prior to the data before performing factor analysis. Results of reliability analysis states that the Alpha value is equal to 0.722 Thus, the research questionnaire can be accepted and can be said to be reliable or trusted as an instrument for collecting research data [10].Furthermore, a factor analysis performed on samples collected research. Confirmatory Factor Analysis (CFA) was done in this study. We create Appendix B that displays the regression results of the factor analysis conducted, these results indicate that B, IM, SU, CO, OP, P, C, AC, A, O, I have a relationship with the latent variables (information security) where the value of P < 0:05 and CR> 1.96, while for the CM, S, H showed no relationship with latent variables (information security) Since the value of P> 0.05 and CR <1.96. From these results thus obtained groups of variables that affect the security of the information that is B (Information Security Aspects of Business Continuity Management), IM (Information Security Incident Management), SU (Supplier Relationships), CO (Communications Security), OP (Operation Security), P (Physical Security), C (Cryptography), AC (Access Control), A (Asset Management), O (Organization of Information Security), I (Information Security Policies).Then to get the significance of variables - variables that can be obtained through standardized before loading factor as in Appendix C. Loading factor latent variable to the observed variables must be greater than 0.50 [11]. Based on the analysis in Appendix C, there are two variables observed as having a loading factor> 0.50 namely OP and AC, it indicates that the OP and AC included into values - core values are determined, so that the OP (Operation Security) and AC (Access Control) the variables that most influence on the latent variables. Evaluation of security operations at PT. IndoDev Niaga Internet referring to the performance targets for IT Support department for the period from July to December 2016 and the results of audits of ISO 27001: 2013 for the period of August 2016. In the performance targets for IT Support department, there are 4 KPI (Key Performance Indicator), namely: System availability, Compliance incidence, IT infrastructure enhancement plan, Ticket resolution time. From the results of the performance of system availability during the period from July to December 2016 it is known that the target of 90% can be achieved during the July-December. This indicate that the performance of the system availability is quite good. The results of performance in terms of compliance incidence during July-December, 2016 was also able to meet the targets set. Performance incidence also includes good compliance. The results of the performance targets for the IT infrastructure enhancement plan, in the period July, August, September, and October did not meet the targets set for July IT infrastructure enhancement plan that is achievable only by 87.5%, and for the month of August amounted to 80%, in September also by 80%, for the month of October by 85%, while for November and December have reached the target of 90% for the months of November and 100% for the month of December, so that the average - average achievement for the IT infrastructure enhancement plan in the period July - December 2016 was 87%, it would still be below the set target of 90%, though below target, but the average achieved is still within the limits of tolerance, so that they are in good category. Scaling back significantly in August and September occurred because the employees of the department who resigned during the period, so there is some plan IT infrastructure enhancement is not running Because of reduced resources needed, but this can be increased in the next period is in October.

The results of the performance of the ticket resolution time during July-August 2016 of the results obtained during this period nothing to meet the target, during that period the average - average obtained is 50.86%, and this result is still quite far with the targets set, where the

difference amounted to 29.14% and that means if in one month there are 60 ticket that must be completed on time, only 31 ticket that can be settled in accordance with the SLA (Service Level Agreement) agreed on the amount of the targeted 48 ticket. Through the results of observations conducted on the ticket is assigned to the department IT Support, it is known that during the period from July to December, 2016 there were 511 ticket that must be completed by the department of IT Support.

The majority of the ticket that must be done is related to security operations (backup & restore, malware protection, configuration, file operations, installation, set up a new instance, SSL certification, query support). If the total ticket then there are 269, or about 53% of the total ticket that existed at that period. By dominating ticket relating to operations security, then the performance targets of the ticket resolution time should be a concern for management to be improved, so that the SLA has been agreed can be always achieved, which in turn will affect the operations of security of the company and ensure that the proper process and safely performed for the operation of information processing device in accordance with the scope and policies of the security operations of PT. IndoDev Niaga Internet. From interviews and observations, it is known that some of the causes of the ticket resolution time failed to meet the target are as follows: Lack of supervision of the direct supervisor of the ticket that must be resolved, lack of resources, division of tasks not done well, and less aware of the targets to be achieved. Evaluation of operations security also looked at the results of the audit of ISO 27001: 2013 for the period of August 2016.In audits conducted in the period August 2016, from 12 items of audit checklist relating to the operations of security, there are 5 items in the category of Non-Conformance (not appropriate), while the third item into the category of Conformance (as appropriate), 2 items into the category of observation (need further observations), and two items fit into the category of follow Up (require follow-up). Of particular concern in this evaluation are 5 items that fit into the category of Non-Conformance. Non-Conformance that occur are within the category of minor nonconformities. Of non-conformance that occur are then conducted further investigation and observation to determine the cause of the nonconformity (root cause). For the mismatches that occur in the check item A.12.4.1, A.12.4.2, A.12.4.3 and A.12.6.2 known to occur due to negligence of staff IT support, while for noncompliance with A.12.5.1 happen because documentation is not up-to-date. Non-conformance minor can be defined such that a mismatch does not have a serious impact on information security. Evaluation of access control refers to the results of the audit of ISO 27001: 2013 for the period of August 2016. The results of the audit of the period for matters relating to access control, found that of the 33 items into audit checklist contained 11 items that fall into the category of Non-Conformance (not appropriate), 9 items belonging to the category of observation (need further observations), 2 items in a category follow Up (require follow-up), and 11 items are included in the category of Conformance (as appropriate).In contrast to the results of the audit of the security operations in which discrepancies that occur are all entered into the minor category, the access control of 11 findings of nonconformity occurs, 9 of them entered into a major Non-Conformance. This means, a Non-Conformance that occurs a serious impact on the achievement of information security. Further observation and investigation conducted to determine the cause of such discrepancy (root cause). Non-Conformance that occur in A.9.1.1.1, A.9.1.1.2 and A.9.1.1.3 caused by the same thing, namely because of the procedures outlined in the working document of instruction for access control is not effective, because the approval process is still going outside the system or occur orally, so that from the IT Support difficult to know whether the request has been submitted has been approved by or not. Then to A.9.1.1.4 and A.9.2.5.1 more due to negligence of staff IT support. A.9.2.1.1, A.9.2.1.2, A.9.2.1.3 and A.9.2.2.2 due to a combination of the negligence of staff IT Support and procedures for access control that is in working instruction is not complete and therefore become ineffective, A.9.2.3.1 due to lack of inspection / review of access to shared folders. A.9.2.4.1 due to the absence of documents used to record the change password.

Table 1. Comparison between current achievement and target.

KPI	Target	Current achievement
System availability	>= 99 %	99.63%
Compliance incidence	<= 3	1.67
IT infrastructure enhancement plan	>= 90%	87%
Ticket resolution time	>=80%	50.86%
Operations security conformance	= 100%	25%
Access control conformance	= 100%	33%

From Table 1 it can be seen that for ticket resolution time, operations security conformance, and access control conformance remained well below the target set. For the ticket resolution time issue which led to the collapse reached the target set is due to aspects of IT service management is not maximized, where IT service management refers to planning, provisioning, and management of IT services in the framework of alignment with the business enterprise [12]. Referring to [13] some misunderstandings often occur in the IT service management, misunderstandings, among others, the problem can be solved if established a good relationship with the user, whereas the service antecedent deliver very closely related to the quality of the service itself, because the quality of these services should continue to be evaluated in order to achieve the expected quality. In the model of IT service management there are five major interrelated processes namely Service Level Management, Event Management, Problems Management, Help Desk Management, and Customer Satisfaction Management [13]. These five processes are interrelated and have an effect between one another, if the company is focusing only on some of the processes and ignore the impact of the processes influence each other, then the IT services provided will be disturbed, therefore, on an action plan to do as in Appendix D.
When viewed from the causes of discrepancies that occur in an audit of operations security aspects can be seen that the majority of problems arise due to negligence of staff IT support, in this case means is the aspect of human error.In order to overcome the problem of human error, of course, important to first identify the type of human error that occurred. [14] classify human errors into three groups, namely skill-based errors, rule-based error, knowledge-based error. That where in this case, negligence occurred into the category of skill-based errors, because these errors occur for activities under routine and actually individuals who have the knowledge, skills and experience to do the job properly, but when attention is diverted then this error can occur [15]. This type of error can be quickly and efficiently to be restored, one of the ways that can be taken is through giving feedback [15]. Therefore, the recommendation action plan that can be done as shown in Appendix E.NC Results found in the aspect of access control most of the major discrepancies, as this would threaten the security of the information from PT. IndoDev Niaga Internet if it is not followed up. Root cause this discrepancy happens by human error as the operations of security, but the type of human error that occurs is different, in this case as the problems review the access control is never done, it is not routinely performed, this omission occurred because of a lack of information or knowledge to do it, human error is included into the knowledge-based error [15]. Furthermore, there is also a mismatch happens because the procedures contained in the working instruction ineffective as it did in A.9.1.1.1, A.9.1.1.2, A.9.1.1.3, A.9.2.1.1, A.9.2.1.2, A .9.2.1.3, A.9.2.2.2. Access control is fundamental in information security [16], the procedure of access control must have the following 3 components: Identification, so that access control can be effective, individuals involved should be identified, authentication, identification requires authentication. This is to ensure that the identity used is authentic (used by people who fit), authorization, a set of actions that are allowed for specific authorization.

Referring to the existing problems, it is mentioned that the IT Support team has not been able to determine whether the request is filed in ticketing system has been approved or not, this means that the authentication process cannot be executed properly. Besides, the other thing is access control procedures regarding authorization, which was also found that the review of user

access rights cannot be done because it has no tools for reviewing it. Roled-Based Access Control (RBAC) can be used to manage roles and access rights of the user, rather than giving access only to certain users [17]. By using roled-based, then the company can undertake a review of user access rights more effectively and efficiently [17]. On the other hand, relate to [18],it is a mechanism to transform goal model to business process model. This mechanism could be used to describe business process model in PT IndoDev Niaga Internet . The system architecture has proposed by [19] to anticipate dynamic environment. Therefore, considering this, the action plan recommendations that can be done as shown in Appendix F.

5. Conclusion

Conclusion of this study are:

1.The most influential factor to the security of customer information PT. IndoDev Niaga Internet is a factor access control and security operations.

2.For the audit results ISO27001: 2013 for the period of August 2016, from the aspect of access control, they found 11 check items that fit into the category of NC (Non-Conformance) of 33 check items in which 9 of them in the category of major and two remaining categories minor, while for operations security aspects of the 12 check items, found 5 that goes into the category of NC (Non-Conformance) and everything was included into the category of minor.

3.Recommendation improvements made include improvements to IT Service Management and procedures, to detail can be seen in Appendix D, E, and F.

Appendices

Appendix A. Security indicators

Security control clauses	Indicator	Ref
Information security policies	Information security policy reduces security breaches	[18]
	Provide assurance about the enforcement of the security functions	[19]
	Information security policy is a prerequisite for effective information security	[20]
Organization of information security	Support and guidance from the executive gives a positive value to the preservation of confidentiality, integrity, and availability of corporate information	[21]
	Establishing and documenting responsibility for information security to ensure that there is no violation of responsibility that result in the information security	[22]
	Separation of duties and responsibilities to reduce the risk of errors, theft, and unauthorized changes to information	[8]
Human resource security	Effective information security awareness can improve an organization's information security posture	[23]
	Determination of the employee's responsibility in terms of information security in work rules reduce the risk of unauthorized access to information	[24]
	Provision of information security training for employees can improve awareness and understanding of the threats, risks, and information security policy	[25]
Asset management	Identify the organization and asset protection measures against these assets into the key applications of information security	[26]
	Classification information provides an indication of how to protect and handle information	[27]
	Media management actions to prevent modification, deletion and destruction of the information stored on illegally	[28]
Access control	Access control enables organizations to control and protect the availability, integrity and confidentiality of resources	[29]
	Access control ensures only authorized access of users who are entitled to the system or a particular service	[30]
	Prevent unauthorized access to a system or a particular service	[31]
Cryptography	Cryptography protects information from unauthorized	[32]
	Cryptography protects the confidentiality of information	[33]
	Cryptography ensure the integrity (accuracy) of information	[5]
Physical and environmental security	By setting a secure area and access cards can prevent unauthorized access to documents, equipment or data	[34]
	Clean desk and clear screen policy reduces the risk of information security breaches	[4]
	Line of defense (perimeter) were plated complicate the theft of information assets	[35]
Operations security	*Capacity management is better able to reduce down time and increase availability (availability)*	[36]
	Policy official ban on the use of software (software restriction policy) prevent information leakage, loss of integrity, as well as a violation of intellectual property rights	[37]
	Backup process and tested according to the procedure to cover the possibility of losses due to loss of data / corrupt	[38]
Communication security	Managed network and properly controlled can protect the information stored in the system and applications	[39]
	Segregation improve network security against network so that information security increased	[40]
	The establishment of policies and procedures to protect the information transfer from the information leakage	[41]
System acquisition, development and maintenance	By setting the policy development secure the integrity, availability and confidentiality of the information generated, manipulated and disseminated by the application system can be guaranteed	[42]
	Protection of the data testing is performed with the same controls and procedures as operational data to protect the information from unauthorized access.	[43]
	Change control procedures to change the software used in the operation of information systems ensure that information systems are not disrupted by the change.	[43]

Supplier relationships	Signing an NDA (Non-Disclosure Agreement) with third parties in order to prevent the occurrence of a security breach related to a third party	[44]
	Determination of SLA (Service Level Agreement) in agreement with a third party to make sure that the service in accordance with the level of security and service level continuity	[45]
	Monitoring and review of third party services on a regular basis to make sure the services provided maintain compliance with security requirements and audit	[46]
Information security incident management	Establishment of an information security incident management enables rapid and effective response to information security incidents	[21]
	The experience and knowledge gained from the analysis and resolution of information security incidents can be used to reduce the likelihood or impact of future incidents	[47]
	Reporting information security events quickly and responsiveness made possible a rapid response to the incident to be investigated	[48]
Information security aspects of business continuity management	Business Continuity Planning ensures availability (availability) when the incident occurred	[49]
	System redundancy sufficient and appropriate to the needs of being able to maintain the system to keep it running	[6]
	Testing business continuity plan regularly to ensure the provision of roles and responsibilities are appropriate when the incident occurred	[31]
Compliance	Legislative requirements, legal or contract for any information system should be explicitly defined	[50]
	Implementation of controls to ensure compliance with the rules relating to intellectual property to protect the intellectual property rights of information and software company	[4]
	The protection of government records in accordance with the rule of law can avoid the loss, damage of counterfeiting and unauthorized access	[51]

Appendix B. Regression weights analysis.

			Estimate	S.E.	C.R.	P	Label
CM	<---	InformationSecurity	-.161	.801	-.201	.841	
B	<---	InformationSecurity	2.752	1.344	2.048	.042	
IM	<---	InformationSecurity	3.542	1.766	2.006	.045	
SU	<---	InformationSecurity	2.580	1.194	2.161	.032	
S	<---	InformationSecurity	-.076	1.296	-.573	.567	
CO	<---	InformationSecurity	6.554	3.078	2.129	.037	
OP	<---	InformationSecurity	12.775	6.423	1.989	.016	
P	<---	InformationSecurity	2.745	1.338	2.052	.031	
C	<---	InformationSecurity	11.473	5.537	2.072	.023	
AC	<---	InformationSecurity	12.733	6.336	2.010	.017	
A	<---	InformationSecurity	1.851	.931	1.988	.048	
H	<---	InformationSecurity	-.102	.951	-.685	.493	
O	<---	InformationSecurity	3.795	1.929	1.967	.041	
I	<---	InformationSecurity	1.909	.923	2.068	.046	

Appendix C. Standardized Regression weights analysis.

			Estimate
CM	<---	InformationSecurity	-.022
B	<---	InformationSecurity	.007
IM	<---	InformationSecurity	.142
SU	<---	InformationSecurity	.080
S	<---	InformationSecurity	-.076
CO	<---	InformationSecurity	.254
OP	<---	InformationSecurity	.675
P	<---	InformationSecurity	.145
C	<---	InformationSecurity	.473
AC	<---	InformationSecurity	.733
A	<---	InformationSecurity	.051
H	<---	InformationSecurity	-.102
O	<---	InformationSecurity	.195
I	<---	InformationSecurity	.109

Appendix D. Recommendation to solved ticket resolution time issue.

Problems	Recommendation
Lack of supervision of the direct supervisor of the ticket that must be resolved	Perform regular weekly meetings to discuss and monitor about SLA realization.
Less aware of the targets to be achieved	
Resources needed less	Doing man power planning in accordance with the estimated work

	load job
There is already a division of tasks in the IT department support, but in execution the division of tasks is less walk, because the assignment of the ticket is done directly by the user and the user himself does not know about the distribution of these tasks	To disseminate returned to the user from another department, division of tasks in IT support staff and make the mapping between the type of work with IT Support staff responsible for such work.

Appendix E. Recommendation to solved operations security performance issue.

Problems	Recommendation
Log Document Review Checklist examined yet have the document number for the period August 2015 and February 2016	The examination should always be done by direct supervisor and things - things that the correction directly delivered and repaired as soon as possible.
There are some server specs are not in accordance with the standards contained in documents.	Routine inspection should be done by direct supervisor to determine whether the spec listed in the document with the original physical was appropriate.
From the samples examined laptop office inventory, they found access to the admin, there should never have admin access.	Conduct periodic audits laptop, to ensure that there is no admin access attached to laptop office inventory

Appendix F. Recommendation to solved access control performance issue.

Problems	Recommendation
Based on the working instruction that has been documented, before the user makes a request to the ticketing system is available, the user must obtain prior approval from certain parties, but at this time IT Support is not able to control whether the request has been approved or not.	1. Revise working instruction, adding owner, admin, as well as approval workflow access. 2. Updating form used. 3. Reviewing access each month and turned into a monthly routine IT Support team
Access Approval process is not appropriate, there should have prior approval from the Technology Development Manager or HR Development only after that access can be granted	
REVOKE access process should be made after reviewing the access control on the form FM-IT-RAC. But the form FM-IT-RAC itself is not valid (inactive)	
Currently, the IT Support has not been able to control whether the request is filed in already approved or not.	
Review access control is never done	Conduct a review of monthly and annual access control for all access control.
Found some errors permissions	
Deregistration process has not always been carried out, they found employees who had resigned but still active domain user whether they are still active	*Update directory user registration and de-registration process.*
Found redundant email account (one employee has more than one email account).	*Update email registration and de-registration process.*
Found users who have resigned or obsolete (not known for certain that account)	
No statement letter to preserve the confidentiality of personal or group.	Formulate a statement letter.
Not yet have the tools to do a review of user access rights and have never done a review of existing user.	Using tools RBAC (Rolled-Based Access Control)

References

[1] A. M. Padyab, "Towards More Structured Information Asset Identification Approach for Risk Assessment Methods," 2013.
[2] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology," 2002.
[3] M. Kazemi, H. Khajouei, and H. Nasrabadi, "Evaluation of information security management system success factors : Case study of Municipal organization," vol. 6, no. 14, pp. 4982–4989, 2012.
[4] R. Thomas, *Information Security Fundamentals, Second Edition*. 2014.
[5] J. Vacca, *Managing Information Security*. 2014.
[6] J. Andress, *The Basic Of Information Security*. 2011.
[7] A. Calder and S. Watkins, "IT GOVERNANCE," 2008.
[8] H. Hai and K.-M. Wang, "The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability," vol. 8, no. 17, pp. 705–716, 2014.
[9] I. 27001:2013, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements," vol. 2013, 2013.
[10] R. . DeVellis, *Scale development: Theory and applications*. Sage, 2012.
[11] B. M. Byrne, *Structural Equation Modeling with AMOS. Second edition*. Taylor & Francis Group, 2010.
[12] M. Marrone, "The Business Benefits of Effective ITSM," 2011.
[13] J. Wan, "Evaluation on Information Technology Service Management Process with AHP," *Technol. Invest.*, vol. 2, no. 1, pp. 38–46, 2011.
[14] J. Reason, *Human Error*. Cambridge University Press, 2010.
[15] D. Embrey and H. Lane, "Understanding Human Behaviour and Error The Skill , Rule and Knowledge Based Classification," *System*, pp. 1–10, 2010.
[16] C. Perrin, "The three elements of access control," 2007.
[17] A. Antonopoulos, "Role-based access control for effective security management," 2011.
[18] Fajar, A.N., Shofi,I.M., (2016).Goal Model to Business Process Model. International Journal of Electrical and Computer Engineering (IJECE) Vol 6 No 6.
[19]. Fajar, A.N., Budiardjo, E.K., Hasibuan , Z.A. "System Architecture In The Dynamic Environment Based on Commonality and Variability Business Processes, 8thICCM, Seoul, 2012