Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs

Ari Kurnianto[1,*], *Rizal* Isnanto[2], and *Aris* Puji Widodo[3]

[1]Magister of Information System, Diponegoro, University, Semarang - Indonesia
[2]Department of Computer Systems Engineering, Diponegoro University, Semarang - Indonesia
[3]Physics Department of Science and Mathematics Faculty, Diponegoro University, Semarang – Indonesia

Abstract. Information security is a problem effected business process of an organization, so it needs special concern. Information security assessment which is good and has international standard is done using Information Security Management System (ISMS) ISO/IEC 27001:2013. In this research, the high level assessment has been done using ISO/IEC 27001:2013 to observe the strength of information secuity in Ministry of Internal Affairs. The research explains about the assessment of information security management which is built using PHP. The input data use primary and secondary data which passed observation. The process gets maturity using the assessment of ISO/IEC 27001:2013. GAP Analysis observes the condition now a days and then to get recommendation and road map. The result of this research gets all of the information security process which has not been already good enough in Ministry of Internal Affairs, gives recommendation and road map to improve part of all information system being running. It indicates that ISO/IEC 27001:2013 is good used to rate maturity of information security management. As the next analyzation, this research use Clause and Annex in ISO/IEC 27001:2013 which is suitable with condition of Data Center and Data Recovery Center, so it gets optimum result and solving problem of the weakness information security.

1 Preliminary

Management is the structure between connectivity and process which is directing and controlling the organization to achieve the goal by giving added value from utilization of information technology to balance and to compare between the risk and the result which is given by information technology and its process [1].

Application of IT management must suitable with business needs and the result which is usually happened in the risk management improvement, communication, and connectivity between business and IT related. Application of IT management is important thing of organization or company which gives direction and control to ensure the significant infestation bringing added value. IT resources become reference of responsibility and mitigation process risk [2].

ISO 27001:2013 is part of management system in an organization based on business risk approach that purposed to build, to implement, to operate, to observe, to maintain and to improve information security. Application of ISO/IEC 27001 allows the organization or company comparing the competition and giving relevant information about IT security [3].

ISO/IEC 27001 known as ISMS (Information Security Management System) is the standard which identifies technical security, but as reality it is a management system, it is not technical standard of information security. There are many organizations or companies assume ISMS implementation is needed by who run in data security only, so it cause lack of awareness for data security in all sectors. To protect information is not only adding device or application, but also all of the process in using application and device must be check, that is why ISMS implementation must be applied in organizations or companies (Broderick, 2006).

ISO 27001:2013 is standard which provides information security management system, the standard is used in the world by organization (commercials and government) as policy management and implementation of information security of organization. ISO/IEC 27001:2013 is designed flexible for stakeholders, internally and externally as the first standing, so the framework can be more focus [4].

* Corresponding author: ari.kurnianto07@gmail.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

The structure of ISO 27001:2013 use management principle which is called as "Deming Cycle" or more known as PDCA (Plan – Do – Check – Action) which is shown at the picture 2.7 [5,6].

2 Methods

2.1 Assessment

In data processing, the result of IT management questionnaire has connectivity to main clause process and annex. The respondents of analysis process are the stakeholders of DC and DRC in population administration information management directorate. The questionnaire calculation procedure is shown below:

1. Every assessment level has attribute processes. Attribute process consists of some criteria which must be fulfilled based on attribute process requirements.
2. Every criteria has assessment score from 1 to 5. The score presented achievement level which is achieved each criteria
3. The next step is accumulation of all the scores have been achieved in each level.
4. The average value must be found by Average the accumulation score.
5. The last step is the average value is divided by the biggest value, and then it is multiplied with 100. The result is categorized suitable with the rules: ISO 270001:2013 requirement haven't been established (not achieved, 0%), ISO 270001:2013 requirement have been established practically (practically achieved, 25%), ISO 270001:2013 requirement have been established overall (largely achieved 50%), ISO 270001:2013 requirement have been established implemented (implemented achieved, 75%) and ISO 270001:2013 requirement have been evaluated effectively (effectively achieved, 100%) [7].

To support IT management audit, the data from questionnaire will be processed and must be done:

1. Calculation of average to each process attribute of all respondent's answer.
2. The assessment is gotten by doing the calculation of all attribute average or processes
3. Existing condition of representation information technology.

The size in the model covers ordinal size and nominal size. The ordinal size is the number which means as level. Nominal size is the number which is used to sort the object from the lowest level to the highest level. The size is not giving absolute value to the object, but it is only giving sort of the level from the lowest to the highest. The next process is to implement between value and absolute value which is done by calculating to be index form using the formula which is shown below :

$$Indeks = \frac{\sum Answer\ the\ questionnaire}{\sum Questionnaire\ question}\ x\ 100\% \quad (1)$$

2.2 Analysis

Information security management system (ISMS) has plan model to assess, the steps to asses is shown at the Figure 1.

Fig. 1. Assessment process ISMS

Determination of assessment activities determine coverage of the thing will be assessed which covers:

1. Obedience to the vision and mission of the organization

2. All of the asset form are the technology form, process, system, service, application, network, and software.
3. The risk assessment covers asset identification, asset definition, asset classification, asset priority, asset determination, control determination, and monitoring.

Gap analysis compares existing condition, whether ISO/IEC 27001:2013 controls have been done well, including policy, procedures, work instruction, till to the documentation. Before doing analysis, first of all the assessment must be done with interview and observation using obedience list assessment direction which is suitable with ISO/IEC 27001:2013.

Table 1. Sensitivity analysis

	Sensitivity analysis	**Assessment point**		
		high (3)	**Medium (2)**	**Low (1)**
confidentiality	How big disadvantage will rise if the disturbance is happened?	if disadvantage is very big and disturb IT services which cause very confidential information leak.	If disadvantage is not significant	If disadvantage is small
Accuracy	How big disadvantage will rise when the disturbance is happened to IT service which is caused by miss using of the data?	if disadvantage is very big and disturb IT services which cause very confidential	If disadvantage is not significant	If disadvantage is small
Availability	How big disadvantage will rise when the disturbance is happened to IT service which is caused by unavailability?	if disadvantage is very big and disturb IT services which cause very confidential	If disadvantage is not significant	If disadvantage is small

The next step by doing risk assessment plan, this step consists of some risk assessment steps, such as:

1. Doing asset identification
   Asset in sub directorate of DC and DRC management in the ministry of internal affairs.
   a. Asset : OceanStor 18000 Series-Storage Rack Exp(4U)
      Classification : hardware
      Sub classification : Storage
      Serial Number : 210211431510FB000002
      Description : -
      Sub location : B1

   b. Asset : SAS Disk Unit(3.5")
      Classification : Hardware
      Sub classification : Hardisk
      Serial Number : 210235875110FB000230
      Description : 600GB 15K RPM
      Sub location : B1

   c. Asset : Disk Enclosure
      Classification : Hardware
      Sub classification : Hardisk area
      Serial Number : 210235877910FB000009
      Description : (4U,3.5",AC,DAE12435U4)
      Sub location : B1

   d. Asset : Disk Enclosure
      Classification : Hardware
      Sub classification : Hardisk area
      Serial Number : 210235877910F9000066
      Description : (4U,3.5",AC,DAE12435U4)
      Sub location : B1

2. Risk determination

   Risk determination of asset refers to confidentiality level, accuracy, and availability. Criteria of critical asset assessment is shown in table 2.

3. Determination of risk priority
   Risk assessment is done using possibility assessment criteria and, effect, and risk value calculation as shown in the table 2.

Table 2. Likelihood scale

Threats	(T1) threat of natutal disaster	(T2) threat of operational disturbance in weakness information security	(T3) threat of hardware	(T4) threat of software
Very seldom	>3 years probability <20%	Very minimum, more than 1 years	Very minimum, more than 1 years	Very minimum, more than 1 years
seldom	between 1- 3 years or probability 21% - 40%	Average is once a year	Average is once a year	Average is once a year
Can be	between 1- 3 years or probability 41% - 60%	Average is once per 6 month	Average is once per 6 month	Average is once per 6 month
often	In 1 years perhaps with probability 61% - 80 %	Average is once per 3 month	Average is once per 3 month	Average is once per 3 month
Very often	Very possible happened in 1 or probability 81%- 100%	Average is once a month	Average is once a month	Average is once a month

Table 3. Impact scale

	Effects	
	(E1) disadvantage of yearly income effect	(E2) reputation effect and law
Not significant	Don't give effect	Don't give effect
low	< (less than) 0.1 % or profit before bank interest, tax,depreciation and amortitsation <0.1%	Complain via communication media (telepon/email/ fax)
medium	between 0,1 % - 1% or disadvantage before bank interest, tax, depreciation, and amortization 0.1 - 1%	Bad reputation PIAK in user perspective, specially electronic identity.
high	between 1 % - 10% or disadvantage before bank interest, tax, depreciation, and amortization 1 - 10%	Bad publication in local media (news,news papper)
critical	More than 10% or disadvantage before bank interest, tax,depreciation, and amortisation >10% or income lost >2%	Bad publication in national media (news,news papper) or law inforcement

The formula of risk calculation criteria shown below:

$$Risk\ value = K\ x\ D \quad (2)$$

Risk value = the result of risk value
K = tendency or possibility
D = effect

Risk value criteria
1. Value 0-5 = low (L)
2. Value 6-15 = medium (M)
3. Value 16-25 = high (H)

The matrix which is used to see the risk value is divided into 3 level; high, medium, and low. The matrix is shown in the Table 4.

Table 4. Risk matrix

		impact				
		1	2	3	4	5
likelihood	1	L	L	L	L	L
	2	L	L	M	M	M
	3	L	M	M	M	M
	4	L	M	M	H	H
	5	L	M	H	H	H

4. Control development
   In the control development step, this step identify existing controls in information security assets, and it is developed to get control which will decrease the incident will be appear.

5. Making road map
   After getting risks which should be fixed, the next step is choosing control that will be used to decrease the risk. When determination of control, it is gotten vulnerability, threat, and effect.

Table 5. Determine of controls

Vulnerability	Control of ISO 27001:2013	Work planning	Code
Disobedience to all of information security process	Management Direction for Information Security	Making rule of implementation and period implementation review to information security policy.	T2
Vulnerability in new employee recruitment	Prior to Employment	Making procedure for new employee recruitment	T2
Minimum awareness of stakeholders and other related people	During Employment	Determine and define responsibility of awareness to information security	T2
Vulnerability of loosing asset	Responsibility for Asset Management	Making procedure for asset borrowing and pointed person in charge (PIC)	T2, T3
Vulnerability of malware attack to DC	Protection from malware	Making procedures to handle, and prevent from virus or malware.	T1, T2, T4, E1, E2
Vulnerability of disaster to DC	Backup	Making back up mechanism to related document and back up testing.	T1, T4, E1, E2

3 Result and Discussion

Data processing in application of information security management system based on ISO/IEC 27001:2013, its assessment process depend on the result of observation and evidence which is saved by the organization. Its process is shown at the Figure 2.

After assessment process has been finished, the result of main clause is gotten and the control has been determined shown at the Figure 3.

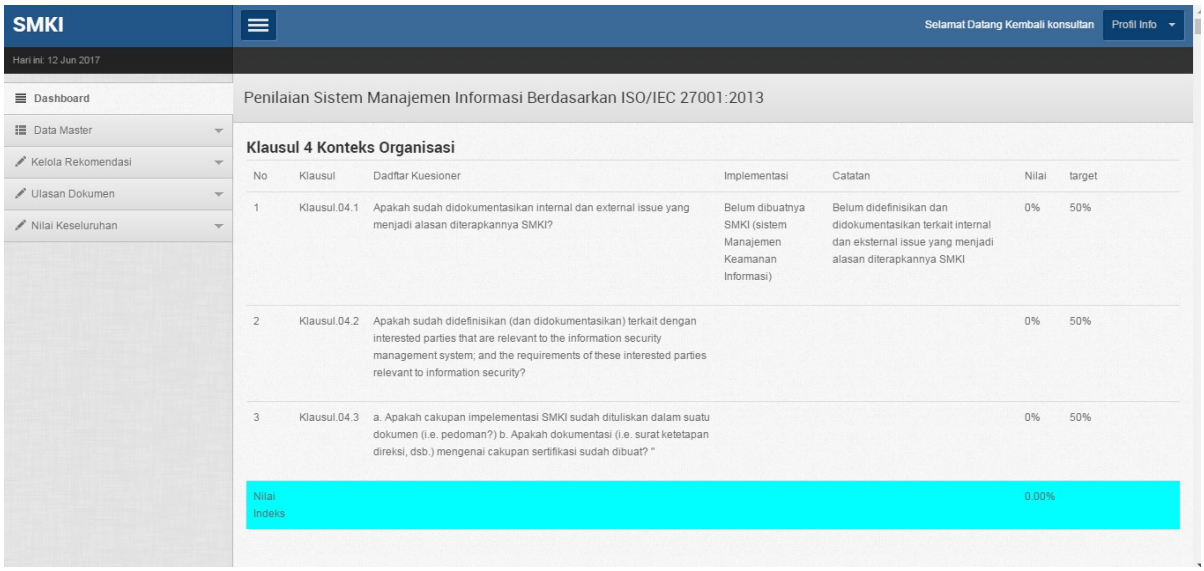

Fig. 2. Results review document and assessment

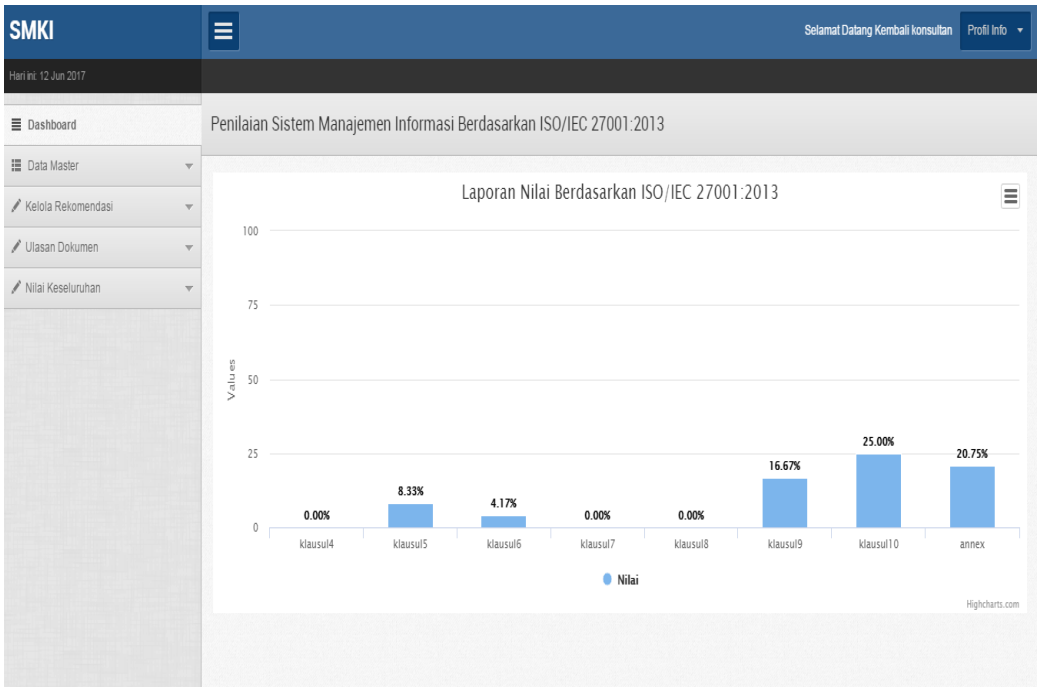

Fig. 3. Results assessment graph score ISO 27001: 2013

4 Conclusions

Assessment of information security management system using ISO 27001:2013 in data center and data recovery center become optimal by choosing control. It is proved with some main clause process and control which is located in sub directorate of management data center and data recovery center still has lack of information security and it must be improved periodically.

References

1. Andriaole, S.. IGTT Governance in the Trenhes. **57-62** (2016)
2. E. Bilbao, A. Bilbao , K. Pecina, and R. Estremera, Physical and Logical Security Management Organization Model Based On ISO 31000 and ISO 27001. IEEE, **1-5**, (2011).
3. E. Bilbao, A. Bilbao , K. Pecina, Physical Logical Security Risk Analysis Model. IEEE, **1-7**, (2011).
4. GEIT, Global Status Report on the Governance of Enterprise It. USA: ISACA, (2011).
5. M. Gerber, and Solms, R. v. Information Security Requirements - Interprenting at Legal Aspects. Computers & Security, **124-135**, (2008).
6. E. Humphreys, Information security management standards: Compliance,. Information Security technical Report , **247-255**, (2008).
7. C. Pelnekar, Planning for and Implementing ISO 27001. Journal ISACA, **1-8**, (2011).