Journal of Theoretical and Applied Information Technology
15th January 2018. Vol.96. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AUDIT INFORMATION SYSTEM RISK MANAGEMENT USING ISO 27001 FRAMEWORK AT PRIVATE BANK

EKIN KABAN, NILO LEGOWO
Information System Department, BINUS Graduate Program-Master in Information System Management,
Bina Nusantara University Jakarta Indonesia 11480
E-mail: kabanekin@gmail.com, nlegowo@binus.edu

ABSTRACT

Control of risk management information systems in the developing world is currently needed to improve performance and provide a very important impact for users of information systems, especially to promote business focus on information systems. Therefore, the perpose of the research it will conduct an audit of risk management information system at private Bank to determine the level of maturity level that has been applied whether it is in accordance with Methodology using ISO / IEC 27001 standard. The process to be used in this risk management information system audit focuses on annex 7. Asset Management, annex 10. Communication and operation and annex 11. Access control. The result of the stages that will be done is from seeing the current condition to the conclusion that results from the maturity level the relevant bank. From the results obtained, the maturity level of asset 7 asset management 3.2, annex 10 communications and operation 3.9 and aneex 11 access controls is 3.7. To increase the value of the maturity level of the bank, a process that must be carried out includes: There are several procedures and compliance that have not been executed by Bank in the overall control of the management asset. the conclution of the research obtained is 3.2 for the maturity level scale of 5 which means there is a gap of 1.8 for the value of compliance to achieve target 5. But, to achieve target 4, Bank has gap analysis 0.8 to get level 4 in maturity Level. To get these levels, things that must be run can be seen in the sub suggestion on the next page. In annex 10 that discuss the Communication and Operations Management, the Bank already done well and in accordance with the existing SOP at the bank. From a scale of 5, the bank has applied maturity level with point 3.9 which can be interpreted that the gap in the annex is 1.1 to get level 5 on the maturity level. To get level 4, Bank must do a little development because the diffrence value from maturity level from 3.9 to level 4 is 0,1. So, it can be ascertained with the compliance and the existing documents in Bank can be run entirely to get the appropriate results for the future. In annex 11 that discusses the Access Control on Bank, it is very good and in accordance with SOP and the standards applicable to Bank. The bank. From the implementation of Bank get maturity value 3,7. To get maturity level 4, then the gap is 0.3. For the future can be maturity level 4 if the process and procedures on sub suggestions can be run properly and correctly.

Keywords : *Audit IS , Risk management , Asset Management , Bank , ISO 27001*

1. INTRODUCTION

Risk is the process of identifying, measuring, monitoring and developing other ways of handling risks, monitoring and controlling in handling risks.

The risk identification done in a company is to assess the extent of the risk that has been executed in accordance with existing procedures and see the extent of vulnerability that occurs if the application is not applied in a company. To that end, many companies are already applying information system security from threats and also the destruction of data that the company has.

ISO 27001 is the standardization of information system security that can be used by the company in the implementation of information system security (SKMI). ISO 27001 has eleven controls that can be applied in an organization or company that can be viewed from the existing control side to maximize the security of information systems that exist in the company.

ISO 27001 has four life cycles that must be run in a company to be able to analyze things that can be used as a reference to maximize SKMI. These are the four life cycles in question:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Plan (Determination of the ISMS): Establish appropriate SKMI policies, objectives, processes and procedures for managing risks and appropriate results With overall organizational policies and objectives.

Do (Application and operation of SKMI): Implement and operate SKMI policies, controls, processes and procedures.

Check (Monitoring and Assessment of SKMI): Assess and, where applicable, measure the performance of the process against the policy, SKMI objectives and practical experience and report the results to management for assessment.

Act (Improvement and maintenance of SKMI): Takes corrective and preventive measures based on internal audit results of SKMI and management reviews or other relevant information, to achieve continuous improvement in SKMI [10].

Management is a technique owned by people to provide direction, influence, supervise and organize the components - components that exist and show each other to be able to achieve the intended purpose is predetermined [7].

Risk is the process of identifying, measuring, monitoring and developing other ways of handling risk, monitoring and controlling in handling risk [3].

From the formulation of the problem above, the purpose of the research is as follows:

To ensure that the custody of assets is properly arranged and recorded in accordance with the SOP applicable to the Bank.

To monitor access controls that are in accordance with SOP in Bank.

To see the extent to which the communication and executed in accordance with the provisions of information system security at Bank.

2. LITERATURE REVIEW

Information is a news that can be considered important if the information is useful for the benefit of an organization or company that needs it. Conversely, information is considered unimportant if the company does not need information (6).

Information Systems is a report required by a company to enhance operational activities and strategies within a company and be documented if at any time it is recovered for the benefit of a company concerned.[5]

Management is a technique owned by people to provide direction, influence, supervise and organize the components - components that exist and show each other to be able to achieve the intended purpose is predetermined. [10]

W. Stallings says these are some of the possible threats to be found [11] :

1. Interruption is damaged data caused by attack directed from system availability (denial of service attack).
2. Interception is an unauthorized party or unauthorized access to assets information.(Wiretapping)).
3. Modification is an unauthorized person making changes to provide untrustworthy information.
4. Fabrication (Fraud) is where unauthorized parties insert fake objects into websites or databases for and deliver messages that are inconsistent with the content of the website. (Including fake messages via computer network).

Debra box and Dalenca Pottas in a journal entitled A model for information security compliant behavior in the healthcare context (2014) said that the health threats of information systems security are[2]:

1. Lack of security sense is due to lack of SOP implementation of the company being built.
2. Users of information systems take risks that exist due to ignorance of existing risks.
3. The act of intentional, negligence or not knowing about the activities that apparently risk impact on information systems are interconnected.

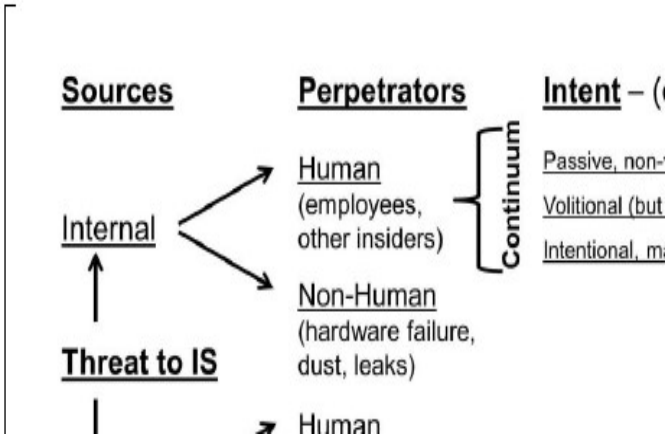

Figure 1 Information Security Threat Vector Taxonomy Abridged – Sourced [7]

2.1 Stage of Risk Management

To determine whether the risk is within the range of dangerous levels or not, it must be done several stages of risk management within an

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

organization or company. These are some of the stages of risk management:

Investigation is to review the information system that has been used if there is a problem and will become an obstacle in the progress of running the business.

Development is the stage after conducting an investigation in a company that uses information systems as a supporter of business progress. This stage will be seen whether the information system used to be done developers or not.

Implementation is a step taken as the development has been reviewed. If at the development stage there is improvement of information systems, it will be done related to the implementation of information system development that has been done before.

Operation and maintenance is where the implementation stage has been performed and at this stage all maintenance related to the implementation of the information system has just been added or improved at the implementation stage.

This settlement is the last stage after the stages of care of the new information system has been implemented correctly and in accordance with the SOP in a company. Risk Evaluation and Mitigation Strategies.

The workflow should conduct a review to be performed by the information security team prior to being given a report to management for approval. The security team may also alter the results of the risk evaluation based on the existing
impacts and once discussed by the company management team and approved by the parties concerned. Evan Wheeler, 2001 in a book published "Security Risk Management"[12]

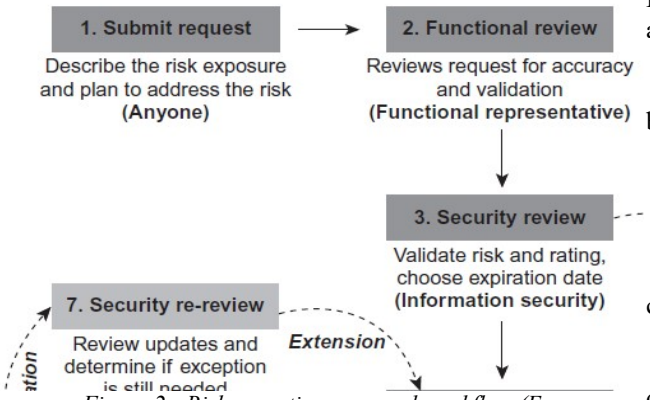

Figure 2 : Risk exception approval workflow (Evan Wheeler ,2001)

2.2 Incident Response life cycle

At this stage will be prepared to train and build a risk management team to be able to detect risks that exist within an organization or company. At this stage the company also limits the number of occurrences that exist for the selection of implementation in a set of security controls based on the results of the risk assessment. But after the implementation period has been run in a company, there will be problems that will arise in the process. An example is when the host adds process is not detected by malware while the process of cleaning the spare malware in the process.

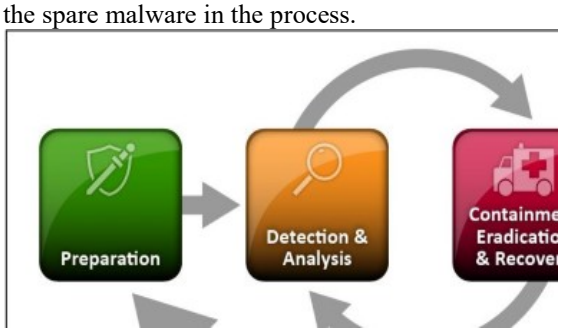

Figure : 3 Incident Response life cycle (Paul Cichonski Agust 2012)

2.3 Preparation

The response of the methodology of events usually emphasizes on preparation and builds the ability to respond to events occurring within the firm to be ready to act on the incidents occurring as well as to ensure prevention of incidents that have not occurred. The established team is also expected to provide basic advice related to handling events and preventing incidents has not happened.

2.4 Detection and Analysis

Perform the existing threats detected and analyze these threats so as not to pose a threat to the company in developing its ongoing business. Events can occur in several ways:

a) External / removeable media: A malicious code spread from flasdisk that has been infected with the virus.
b) Attrition: Attacks that use brute force to degrade system performance or destroy system logos (eg DDos to refuse access to services or applications, brute force attacks against authentication, passwords and digital signatures).
c) Web: Offensive attacks from web-based sites such as scripting to redirect the web to malfunction properly and install malware
d) Email: Attack via email message or email attachment. For example: enter the code into document that has been attached or link to web maliciouse into body email message.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

e) Loss or thief of Equipment: Loss or theft of computer or media devices used by companies such as laptops, smartphones or authentication tokens.
f) Other: Attacks that occur outside of the categories described above.

2.5 Containment, Eradication, and Recovery

this stage is where the stage for containment, eradication and also data recovery will be maintained to be restored. Strategies undertaken by each company will be different - different in the handling of problems that occur. Companies must establish precise criteria in clear documentation to facilitate decision making. The right strategy decision includes several criteria such as:

1. Potential damage and theft of resources.
2. The need for supporting evidence.
3. Availability of adequate services (network connectivity, services provided by external parties).
4. Time and resources needed for strategy implementation.
5. The effectiveness of the strategy (partly containment or full detention).
6. Duration and solution (solution to be removed within four hours, temporary solution to be removed within two weeks and permanent solution).

2.6 Post Incident Activity

This process focuses on improvements that will be made after the information system has been implemented properly and correctly. From this handling, it is expected that information security team can develop to know the handling of problems that have occurred or handling problems that have not happened in order to provide controls in accordance with the security framework used in the company.

If the problems that exist within the company happen repeated, then the life cycle will return to the early phase until post incident acitivity phase to be able to improve and maintain the security of existing information systems within the company well and correctly in accordance with the SOP and framework that exist in the company concerned [8].

2.7 ISO/IEC 27001 Controls and Objectives

Standardization of SNI ISO IEC 27001: 2009 is a standard used for security audit of information systems within a company or organization. These are some of the objective controls and their explanations contained in the standardization of SNI ISO IEC 27001: 2009 to facilitate the selection of scope in running the information system security audit.

Can be described some clauses that exist in ISO IEC 27001: 2009 are as follows:

1. Annex 5 Information security policy.
2. Annex 6 Information security organisais.
3. Annex 7 Asset management.
4. Annex 8 Security of human resources.
5. Annex 9 Physical and environmental security.Annex
6. 10 Communication and operation management.
7. Annex 11 Access control.
8. Annex 12 Acquisition, development and maintenance of information systems.
9. Annex 13 Information system security incident management.
10. Annex 14 Business continuity management
11. Annex 15 Conformity.

Each clause / annex has different needs depending on the needs of the company who want to apply the clause to provide more security so that data and information from the company can not be tapped or taken by unauthenticated people [4].

2.7 Information Security Index

The information security index is a module used to calculate the maturity level of ISO 27001: 2009 standardization to make it easier to look for things that must be maintained, improved and also that must be mitigated because the data process is not in accordance with the applicable SOP in a company.

Evaluation stage is done through a number of questions that each area below:

1. The role of ICT in agencies.
2. Information security governance.
3. Information security risk management.
4. Information asset management and.
5. Information technology and security.

From the module that has been provided, it will be given some questions that will be answered by related parties. To get the real answer, it is expected to answer the questions already provided with honesty and openness. This is to represent what - what should be maintained, improved and mitigated from a company that still has not implemented SKMI in the company.

Journal of Theoretical and Applied Information Technology
15th January 2018. Vol.96. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table : 1 Security status

Status Pengamanan	Kategori Pengamanan		
	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Above is an example table for the security status that will be done by the company that will fill the questionnaire to see the level of readiness / maturity level. For OUR Index purposes, the maturity level is defined as:

1. Level I - Initial Conditions
2. Level II - Implementation of the Basic Framework
3. Level III - Defined and Consistent
4. Level IV - Managed and Teruku
5. Level V - Optimal

To help provide a more detailed description, this level coupled with levels between - I + II + III + and IV +, bringing the total there are 9 levels of maturity. As a start, all respondents will be given a first-level maturity category as equivalent to the standard ISO / IEC 2700: 2005, the level of maturity that is expected to be a minimum threshold of readiness certification is Level III +.
From this picture it is explained that there are levels in determining the risk management that exist within an organization of course different or different will not the same level of risk that exist for all divisions of that company. Of this figure will be explained that if a company is on the scale:

a) Low: 0 - 12
b) Moderate : 13 - 24
c) High : 25 - 36

Table : 2 Risk mapping table for exceptions

		Severity	
		High	Moderat
ikelihood	High	High	High
	Moderate	High	Moderat

2.8 Maturity Level CMMI

Maturiy level is a tool to measure how mature level achieved by a company in the application of information system audit. For that, then these are the levels that can be seen from each level in the CMMI framework for calculating the level of maturity in a company or organization:

According CMMI, these are some models of maturity level level of CMMI model:

1. Level 1 (Initial):

The criteria of the initial level in maturity level are:

a) No project management
b) Absence of quality assurance
c) The absence of change management mechanisms (change management)
d) No documentation

2 Level 2 Repeatable

The characteristics of the repeatable level are:

a) Software quality begins to depend on the process rather than on people
b) There is a simple project management
c) There is a simple quality assurance
d) There is a simple document
e) There is a simple configuration management software
f) The absence of knowledge management
g) Absence of commitment to always follow SDLC under any circumstances
h) Absence of stastal control for project estimation
i) Vulnerable organizational structure changes

3. Level 3 Defined

The characteristics of the Defined level for CMMI are:

a) SDLC has been determined
b) Commitment to follow the SDLC under any circumstances
c) The quality of processes and products is still qualitative or only approximate
d) Not apply Activity Based Costing
e) The absence of a standard feedback mechanism.

4. Level 4 Managed:

The characteristics of Managed Level in maturity level are:

a) There is already Activity Based Costing used for the next project estimate
b) The process of quality assessment of software and projects is still quantitative
c) There is waste of costs for data collection because the data collection process is still done manually
d) Already have feedback mechanism
e) There is no defect prevention mechanism

Journal of Theoretical and Applied Information Technology
15th January 2018. Vol.96. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. Level 5 Optimized:

Optimized Level features in maturity level are:

a) Automatic data collection
b) The existence of defect prevention mechanism
c) The existence of a very good feedback mechanism
d) Increasing the quality of human resources and also improving process quality.

At level 5, continuous process improvement is the way of life. The focus is on preventing the occurrence of defects and encouraging innovation. In an immature organization, no one may be responsible for the repair process. A mature organization usually has 70-80% participation in improvement activities at any time and every person involved. Continuous process improvement means controlled changes and improvements are measured in process capabilities [9].

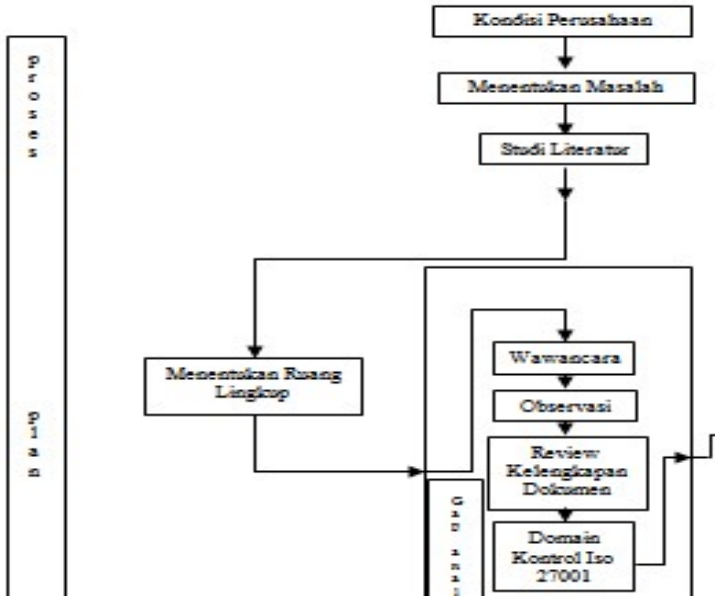

Figure 4 : Framework of Think

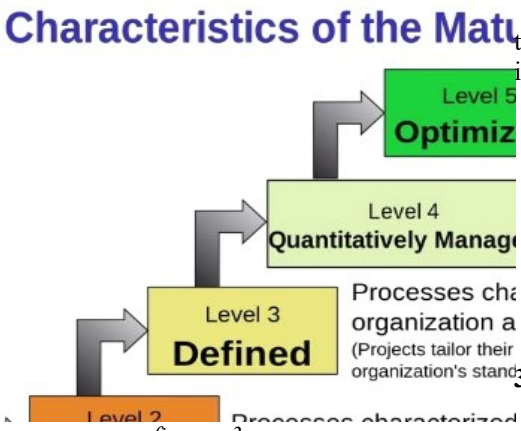

figure : 3
https://commons.wikimedia.org/wiki/File:Characteristics_of_Capability_Maturity_Model.svg

3. METHODOLOGY

From the formulation of the problem described in chapter 1.2, the frame of mind of report writing is about the issue of ISO 27001 Management Survey with annex 7 domain focusing on asset management and also annex 11 focusing on access control. Of all sub - sub that exist in annex7, annex 11 and annex 11, which will be calculated maturity level of all existing processes in PT Bank.

From the description of the picture above, then this is the step - step of the frame of mind that is done on the Bank:

1. Determining the Problem
2. Literature Studies
3. Determining the Scope
4. Gap Analysis
5. Risk Assessment
6. Setting Controls
7. Policies and Procedures
8. Statement of Applicability

3.1 Data Analysis Technique

In this thesis research, it will be done data collection techniques from related parties ie Bank to be processed and calculated from the results of questionnaire analysis and session wawanca whether it is in accordance with bank SOP PRIVATE and ISO / IEC 27001: 2009 standard. The questionnaire will be given around the application of ISO / IEC 27001: 2009 which focuses more on annex 7 asset management, annex 10. Communication and operational and annex 11. Access control. The method used is to use the information security index (WE) method.

At the information security index stage (WE), there are several levels that can be seen from processes such as:

1. Level I - Initial conditions.
2. Level II - Implementation of the initial framework.
3. Level III - Defined and consistent.
4. Level IV - Managed and structured.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

• Level V - Optimal.

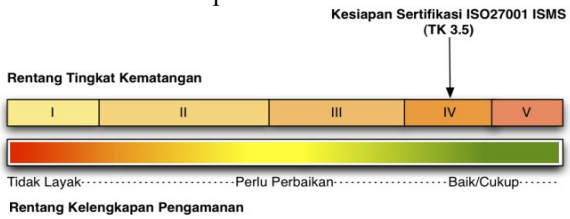

Figure 5 The Maximum of Security Gap (Irawan Afrianto dkk) [1].

The scope of the research for the author's thesis report is as follows 3 of 11 from framework ISO 27001:

1. Annex 7
2. Annex 10
3. Annex 11

3.2 Annex 7 Asset Management

Annex 7 Asset management: This is about managing assets in the company. This asset includes parts of all physical and non-physical things when it is priced and useful, it will be said to be assets by the company. Assets that include from Bank will be given a questionnaire to see the list of assets that the company owns.

3.3 Annex 10 Communication and Operation Management

In Annex 10, which focuses on communications and operational arrangements, this material is more focused on what will be delivered in a company to dalpat communicate well and correctly in accordance with SOPs that exist in Bank and also how the operational arrangements can run with existing SOPs.

3.4 Annex 11 Access Control

From Modules that focus more on access controls that exist within an organization or company, then these are some sub - sub modules that exist in annex 11 access control such as:

To determine the level of maturity of a company, the authors should look for evidence as complete as SOP, company data, questionnaire results and interviews if necessary to ensure all information system security has been executed properly and correctly in accordance with ISO 27001 standards.

4. DISCUSSION

4.1 The results of the Information Systems Security Index

This is the result of our index that has been filled by the Bank to see the extent of the bank's readiness for securing information systems that exist in Bank. In the index information security system itself, is divided into six sections each - each section has its own knowledge about the application of information systems within an organization. For more details, it will be described as the main points to be able to see in detail what parts should be improved and which parts need to be maintained and improved for the future.

4.2 Part I The Role of ICT

This section looks at how ICT roles and ICT level of interest in agencies have been going on so far and it can be seen how important the role of ICTs in an organization is to improve and promote ongoing business. Whether with the application of ICT in a company can give a more significant impact or does not give any meaning in the company.

4.3 Part II Governance

This section discusses how the governance of information system security is in Bank. The total evaluation value in this section that covers the information security governance can be seen in the OUR index.

This section evaluates the readiness of the form of information security governance and the agency / functions, duties and responsibilities of information security managers. Bank achieves the total value of governance evaluation on the number of values reaching 76 points that is intended is that most of the existing process has been implemented in part and also there are some statements that have been established as a whole.

4.4 Part III Risk

In this section it can be seen how far the Bank evaluates the readiness of the implementation of information security risk management as the basis for the implementation of information security strategy. From the following figures can be seen on the results of the implementation that has been run on the Bank.

The total value of the information security risk management evaluation that is in Bank is 31 points from the total score score of the application phase of the first and second sections on the OUR index.

4.5 Part IV Framework

This section evaluates the completeness and readiness of the information security management (policy & procedure) framework and its implementation strategy

The total value of the evaluation of working kerangaka that has been filled by Bank is 120 points, most of the procedures and policies of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

bank has been implemented in part and has been implemented thoroughly.

4.6 Part V Asset Management

This section evaluates the completeness of securing the information assets, including the overall cycle of use of those assets. In Bank, asset has been done well and also there are regulators who arrange it is called with IT ORM SKAI division. There are already SOPs who have taken up the matter. From the OUR index framework, the total evaluation value of the existing asset management at Bank is 114 points which can be interpreted that The status of the implementation has been applied in whole and partially implemented.

4.7 PART VI Information Technology and Security

This section evaluates the completeness, consistency and effectiveness of the use of technology in securing information assets. Bank has been applying well on information technology and security when viewed from the spreadsheet on the index. The total value of technology evaluation and information security is 101 which mostly has been applied thoroughly by Bank to maintain the assets and also the data that exist in Bank for the sustainability of business run at the bank.

4.8 OUR Index Dashboard

Dashboard OUR index describes the sequence of the entire activity from the beginning to the end on the index chart WE and will form a spider diagram to look over towards where the application of existing information systems security in a company.

For more details, the authors put the images for viewing on the system information security dashboard on our index.

Figure 6 : Sum of Information System Index

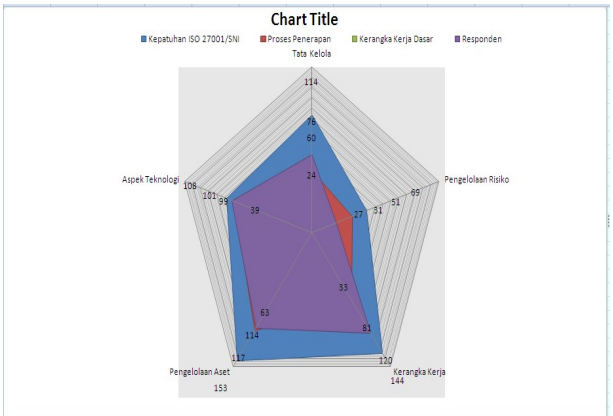

Figure 7 : Gap Analysis

The Result of Index information System Gap analysis is the need to see and compare the extent to which processes are already implemented within an organization to see which data and processes in ISO 27001 have been done in terms of policies, procedures, instructions and also documentation in every process that exists within the company. For that before the author did the analysis gap, the first thing to do is do a gap assessment. The following is a gap assessment between interviews, observation with gap analysis guidelines and ISO 27001: 2013 tool audits.

Interview

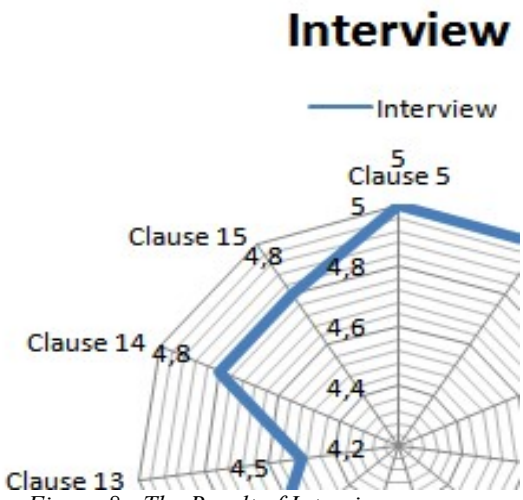

Figure 8 : The Result of Interview

From the picture above, it can be explained that the outcome of the interview to Bank has been very good because it is already some control at the level of 4 and have already reached level 5, which means to position the views of ISMS is very good because it is already doing the application in accordance with the SOP and Policy of OJK and

Journal of Theoretical and Applied Information Technology
15th January 2018. Vol.96. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

also BI. For more details, an observation will be made to compare whether the results of the interviews and observations are valid with the data in accordance with the ISO 27001 assessment checklist.

Observation

For the observations that have been done on the Bank can be seen in the picture above that can be seen from the blue line stating the evidence of observations on the Bank. For red line is for ISMS compliance value of ISO 27001 standardization that is max at level 5. After mapping between interview and observation, then the mean of compliance value applied to Bank is 3,5 - 3,9 which means That the ISMS applied is well executed and in accordance with the procedures of Bank and also from the regulation of OJK and Bank BI.

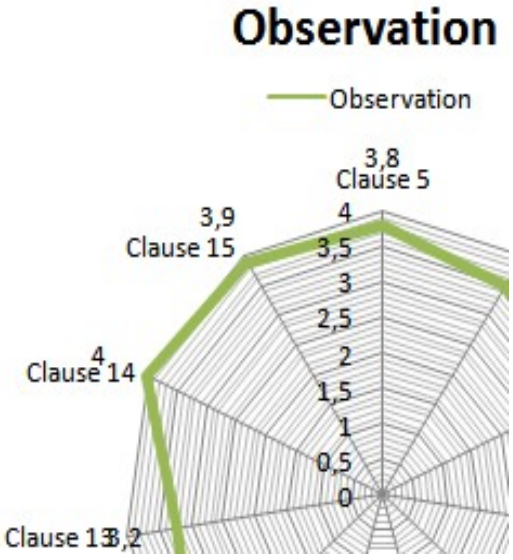

Figure 9 : The Result of Observation

ISO 27001 Control Objective

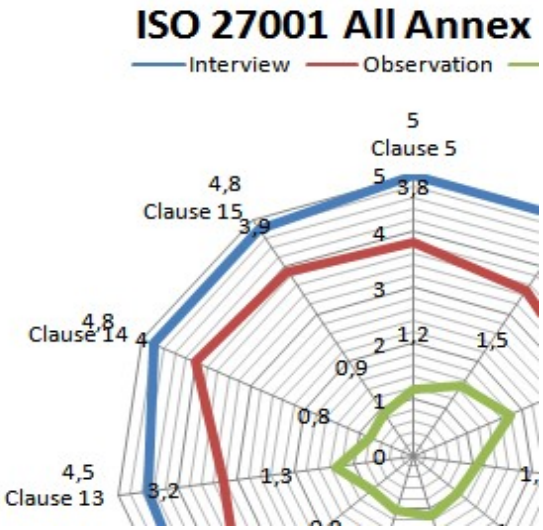

Figure 10 : Clause ISO 27001 Spider Chart

From the picture above, it can be seen that the image is a combination of all the controls in ISO 27001 ISMS.Untuk description of each color, can diliat from the description that already exists in the picture above. For the picture above it is clear that for the green line is the result of the gap of the existing analysis on the Bank. It states that for all banks PRIVATE has implemented ISMS properly and correctly in accordance with the applicable SOP and in accordance with the regulations of OJK and BI. The green line is the result of an analytical gap which, if from any control and sub controls is executed properly, then the Bank will reach level 5 for ISMS. Furthermore, there will be some suggestions as well as conclusions that can be seen in chapter 5 for conclusions and suggestions. Which will be given the current condition (as - is) and the condition to come (to - be).

Table : 3 Maturity Level ISO 27001

CLAUSE	MATURITY LEVEL
5	3,8
6	3,5
7	3,2
8	3,9
9	3,7
10	3,9
11	3,7
12	3,8
13	3,2
14	4
15	3,9
NILAI MATURITY LEVEL	3,69

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From the results of the gap analysis of maturity level existing in Bank, it can be seen that the expected results for the future is on scale 4 of scale 5 which means that if the Bank wants to be a scale of 4 then the things above must be done by the overall division Is on the linked bank.

According CMMI, these are some models of maturity level level of CMMI model:

- Level 4 Managed:

The characteristics of Managed Level are:

1. There is already Activity Based Costing used for the next project estimate
2. The process of quality assessment of software and projects is still quantitative
3. There is a waste of costs for data collection because the data collection process is still done manually
4. Already have feedback mechanism
5. There is no defect prevention mechanism

At level 4, an organization has achieved all the specific and generic goals that exist at Level 2, 3, and 4. The processes that occur can be controlled and added using measures and quantitative estimates. Quantitative objectives for process quality and performance are defined and used as criteria in process management.

- Level 5 Optimized:

The characteristics of Optimized Level are:

1. Automatic data collection
2. The existence of defect prevention mechanism
3. The existence of a very good feedback mechanism
4. Increasing the quality of human resources and also improving process quality.

In this process an organization has:

Achieving all the specific and generic goals in Level 2, 3, 4, and 5. Optimized levels focus on continuous process improvement through technological innovation.

At level 5, continuous process improvement is the way of life. The focus is on preventing the occurrence of defects and encouraging innovation. In an immature organization, no one may be responsible for the repair process. A mature organization usually has 70-80% participation in improvement activities at any time and every person involved. Continuous process improvement means controlled changes and improvements are measured in process capabilities.

5. CONCLUSION

So the conclusion of information system security analysis that has been done on Bank is as follows:

In annex 7 which discusses the asset management available in Bank can be seen for the maturity level that has been implemented is 3.2 scale 5 which is this gap is quite big compared to the existing gap of the whole annex that has been applied by the Bank. The gap obtained from the implementation result is 1.8 of the total implementation of annex 7 in Bank.

In annex 10 that discuss the Communication and Operations Management, the Bank already done well and in accordance with the existing SOP at the bank. From a scale of 5, the bank has applied maturity level with point 3.9 which can be interpreted that the gap in the annex is 1.1 to get level 5 on the maturity level.

In annex 11 which discusses the Access Control on Bank, it is very good and in accordance with SOP and the standards applicable to Bank. The bank. From the implementation of the Bank has applied 3.7 maturity level from the results obtained interview is 4.7. Therefore, the gap of analysis in Bank is 1.

Bibliography

[1] Ariefianto. (2006). Perencanaan Tata Kelola Keamanan Informasi. Jakarta: Fasilkom UI.

[2] Debra box, D. &. (2014). A model for information security compliant Behaviour in the healthcare cotect. Chicago.

[3] Djohanputro. (2008). Pengertian manajemen resiko.

[4] IEC, S. I. (2009). ISO 27001:2009. Jakarta: SNI ISO.

[5] Laudon. (2010). Information System Management. Jakarta: PT Data Sentosa.

[6] Mcleod. (2007). Sistem informasi Managemen. Jakarta: PT Index.

[7] Oey, L. L. (2010). Pengertian Manajemen. Yogyakarta: Administrasi UGM.

[8] Paul, (2002). Secuity Information system: USA

[9] Rinaldo, Degaz . 2011. CMMI (Capability Maturity Model Integration). http://Degaz Rinaldo CMMI (Capability Maturity Model Integration).htm//. Diakses 07 Maret 2014

[10] Robbins, S. P. (2010). Manajemen. Jakarta: Erlangga.

[11] Stallings, W. (1995). Network and Internetwork Security. Prentice Hall.

[12] Wheeler, E. (2001). Security risk management.