Trikonomika
Volume 17, No. 1, June 2018, Page. 28-37
ISSN 1411-514X (*print*) / ISSN 2355-7737 (*online*)

INFORMATION SECURITY ASSESSMENT USING ISO/IEC 27001: 2013 STANDARD ON GOVERNMENT INSTITUTION

Akmal Zaifullah Maingak
akmalzaifullah@gmail.com
Candiwan
Listyo Dwi Harsono
Faculty of Economics and Business, Universitas Telkom
Jl. Telekomunikasi Terusan Buah Batu, Bandung 40257, Indonesia

received: 21/12/17; revised: 02/01/18; published: 27/06/18

Abstract

The purpose of this research is to determine the existing gap to achieve ISO/IEC 27001:2013 certification and determine the maturity level of the information system owned by X Government Institution. The information system of X Government Institution would be assessed based on 14 clauses contained in ISO/IEC 27001: 2013. The method used is qualitative method, data collection and data validation with triangulation technique (interview, observation, and documentation). Data analysis used gap analysis and to measure the maturity level of this research used CMMI (Capability Maturity Model for Integration). The result of the research showed that information security which had been applied by X Government Institution was at level 1 (Initial) which meant there was evidence that the institution was aware of problems that needed to be overcome, unstandardized process, and tended to handle the problem individually or by case.

Keywords*: ISO/IEC 27001: 2013; information security; CMMI; assessment*

INTRODUCTION

Information is necessarily needed for an institution to decide. Susanto et al (2011) stated that information is a source of organizational life, an important business asset in the world of Information Technology (IT) today. Access to high-quality, complete, accurate and up-to-date information is important in supporting managerial decision-making processes that lead to sound decisions. Institutions will have many benefits if it has an information system that is able to manage information well.

Disterer (2013) argued that information and information systems are an important foundation for companies because more and more internal and inter-company data transfers will increase the risk of threats to information and information systems. Luo, et. al. (2011) stated that information system security management does not only depend on the size of the technology used but also on managerial efforts to manage it. Hu, et. al. (2012) argued that one of the main challenges in information system security management is to understand how organizational, individual and technical factors altogether influence the results of information security in an organization.

By having an information system with a good level of information security, institutional management can easily make management decisions. A decision that is not based on correct information will have a fatal impact on institutional activities to achieve institutional goals. In the management of institutional information security, there is certainly a risk of threats from inside and outside the institution that can harm an institution. Safa, et. al. (2015) confirmed that information security management risk includes two aspects: 1) software and security features, such as pop-up blocking, anti-spyware, and anti-virus software functions; 2) security care awareness behavior related to computer and internet use.

Based on a survey conducted by Cyber Security Breaches in 2016, the types of information security threats that are most prevalent in institutions in the world were viruses, spyware or malware, others impersonating organizations in emails or online, denial of service attacks, etc. In this survey, the most common type of threat to institutional information security is viruses, spyware or malware. Based on complaints obtained by ID-CERT from victims of internet abuse in Indonesia in 2010-2016, the main cause of internet abuse was dominated by spam, IPR, malware, network incident, spoofing/phishing, and spam complaints.

Based on Minister of Communication and Information Regulation No. 4 of 2016 concerning Information Management System Article 4, there were 3 categories of electronic systems based on the principles of risk and their impact, namely Strategic Electronic System, High Electronic System, and Low Electronic System. In the Minister of Communication and Information Regulation No. 4 of 2016 there is also a regulation in article 7 which stated that: (1) The Electronic System Operator that organizes the Strategic Electronic System must apply the SNI ISO/IEC 27001 standard and the security provisions stipulated by its Supervisor and Regulating Sector Agency. (2) The Electronic System Operator that organizes a High Electronic System must apply the SNI ISO/IEC 27001 standard. (3) The Electronic System Operator that organizes a Low Electronic System must apply the Information Security Index guidelines.

Although the above regulations have been issued by the Minister of Communication and Information, there are still many companies that do not apply information security standards to the information systems it has. Abu Saad, et. al. (2011) stated that despite organizational recognition of the importance of implementing information security standards such as ISO 27001, organizations often refrain from doing so because of the higher costs of implementing these standards, and the lack of evidence that these standards have a positive cost/benefit ratio.

X Government Institution is an institution that has the task of organizing affairs in the field of agrarian/ land and spatial planning in the government to assist the President of the Republic of Indonesia in organizing state government. X Government Institution has an information system that can be accessed by government employees and the general public. Of course, it is necessary to manage information systems with very good information security quality to avoid various threats that can damage the X Government Institution's information system. Therefore, a standard is needed to regulate the governance of information security management system of X Government Institution.

To determine the standard, X Government Institution must implement information security standards that are in accordance with Minister of Communication and Information Regulation No. 4 of 2016 article 7, then an assessment of the Electronic System Category is based on the format issued by the Ministry of Communication and Information through the KAMI Index.

Based on the score of the determination of the Electronic System Category obtained by X Government Institution is 32, the X Government Institution is classified as an Electronic System Operator that organizes a High Electronic System. Because the Electronic System of X Government Institution is included in the high category, X Government Institution must apply the ISO/IEC 27001 standard to its Electronic System.

Based on the background that has been stated, the description of the problems to be discussed in this study is that X Government Institution needs to know the current gap information to be able to get ISO/ IEC 27001:2013 certification and also as a public service provider agency, X Government Institution requires an assessment to find out the maturity level of information security owned on ISO/IEC 27001: 2013. The purpose of this study is to determine the existing gap to achieve ISO/IEC 27001: 2013 certification in the X Government Institution information system and determine the maturity level of information systems owned by X Government Institution. In general, research on information security assessment using ISO/IEC 27001:2013 only assesses several clauses, which are around 3-7 clauses, but in this study, we will assess the security of information in accordance with 14 clauses in ISO/IEC 27001: 2013.

Jawadekar (2012) proposed various definitions of information management system, namely: (1) IMS is defined as a system that provides information support for decision making in organizations, (2) IMS is defined as an integrated system of people and machines to provide information to support operations, management and decision-making function in organizations, (3) IMS is defined as a system based on a database of organizations that evolve with the aim of providing information to the community in the organization, (4) IMS is defined as a Computer Based Information System. While Tu and Yuan (2014) argued that information system management is systematic processes that effectively address information security threats and risks in an organization, through the application of appropriate physical, technical or operational security controls, to protect information assets and achieve business objectives.

To get a better grip on information processing activities, Jawadekar (2002) stated that a formal system is needed that must be met by the organization by considering things such as handling large amounts of data, confirming data and transaction validity, complex data processing and multidimensional analysis. fast search and data retrieval, mass storage, information system communication to users on time, and meeting changes in information needs.

Information Security Management System (ISMS) is needed in the implementation of organizational information security. There are several definitions of the information security management system, one of which was put forward by Chazar (2015) who stated that the ISMS is a systematic approach to establish, implement, operate, monitor, review, maintain and improve information security for organizations to achieve business goals. Whereas according to Islami, et. al. (2016), Information Security Management System is a system that combines analysis and design methods, information system users, community managerial problems and

ethical problems. The above definition showed that the security system includes a broader perspective compared to computer security (technical oriented).

The security plan will contain the determination of the combination of information security controls that are used, as well as the priority in implementing them. The basic content on information security plan documents (information security plan) according to Islami, et. al. (2016) were threats and weaknesses, goals and objectives, rules and responsibilities, and strategies and security controls.

There are various definitions of information security, one of which is the definition proposed by Islami, et. al. (2016) that information security is an effort of all members of the organization to protect information from various threats to ensure business continuity, minimize damage due to threats, and accelerate the return of investment and business opportunities.

Another definition of information security was put forward by Sarno and Iffano (2009) who stated that information security is safeguarding information from all possible threats in an effort to ensure/ guarantee business continuity, reduce business risk and maximize/accelerate return on investment and business opportunities. Whereas Whitman and Mattord (2014) argued that information security is information protection and its critical characteristics (confidentiality, integrity, and availability), including systems and hardware that use, store, and transmit such information, through the implementation of policy programs, training and awareness, and technology.

The critical characteristics of information according to Whitman and Mattord (2014) were, confidentiality, integrity, availability, personal, identification, authentication, authorization, and accountability. Of the eight characteristics described by Whitman and Mattord, Sarno and Iffano (2009) argued that information security only covers the first three critical characteristics, namely: Confidentiality, Integrity and Availability.

There are various definitions of ISO/IEC 27001:2013, one of which is the definition proposed by Surya and Sulistyono (2016) namely ISO/IEC 27001:2013 is a special method that is structured about information security that is internationally recognized. Beckers, et. al. (2013) stated that ISO 27001 defines the requirements for establishing and maintaining ISMS and specifically this standard describes the process of making a model of all business risks of a particular organization and specific requirements for implementing security controls.

Whereas Dewi, et. al. (2017) stated that ISO/ IEC 27001:2013 is a standard Information Security Management System (ISMS) standard document that provides a general overview of what should be done in an effort to implement information security concepts in an institution. Candiwan, et. al. (2016) argued that ISO/ IEC 27001: 2013 is an information security standard that explains the requirements for creating, implementing, implementing, monitoring, analyzing, and maintaining and documenting ISMS standards. Beckers, et. al. (2014) stated that ISO 27001 standards are compiled based on the "Plan-Do-Check-Act" (PDCA) model. In the Plan phase, ISMS is designed, in the Do phase, ISMS is implemented and operated, in the Check phase, ISMS is monitored and reviewed, and in the Act phase, ISMS is maintained and enhanced.

ISO/IEC 27001:2013 is the latest revision of ISMS (Information Security Management System) issued in October 2013 by ISO (The International Organization for Standardization) and IEC (The International Electrotechnical Commission). Candiwan, et. al. (2016) stated that there are 14 Main Clauses, and 114 controls in ISO/IEC 27001:2013 presented by the National Standardization Agency that can be applied to build ISMS.

To identify the maturity level of information security application with ISO/IEC 27001:2013 standards in this study required maturity model. Al-Mayahi and Mansoor (2012) argued that the concept of maturity model is regularly used in the field of Information Systems as an approach to organizational assessment. Any systematic framework for benchmarking and improving performance that has a continuous improvement process, can be considered as a model of the level of engagement. This study refers to the maturity model used by the COBIT (Control Objective for Information and Related Technology) framework or CMMI (Capability Maturity Model for Integration).

Komalasari and Perdana (2014) revealed that CMMI is a maturity model that is used to assess IT management more efficiently which can be applied to each ISO/IEC 27001:2013 clause. For the management of identifiers, the application of information security levels applied by the organization is based on the model of maturity levels ranging from level 0 (non-existent) to level 5 (optimized). The purpose of the maturity level model is to find out the existence of existing problems and how to determine the priority of improvement. The CMMI maturity level is generally shown in Table 1.

If grouped based on the value of the maturity level, it can be detailed as in Table 2. The use of maturity model allows management to identify current institutional conditions, current industry conditions for comparison, conditions desired by the institution, and desired growth between as-is and to-be.

METHOD

This study uses a qualitative approach to explore the object of research with a series of interview procedures with related parties. This study uses triangulation techniques with technical triangulation types. Engineering triangulation research used interviews, observation and documentation for the same data source simultaneously.

The results of interviews, observations and documentation were included in the work paper gap analysis. Gap analysis was done to compare the performance of information security that had been applied by the object of research with information security standard of ISO/IEC 27001:2013. The results of the work paper gap analysis were assessed into the maturity level assessment, can be seen in Table 3.

RESULT AND DISCUSSION

Data was analyzed with the first step to reduce the results of interviews, summarized the data of observations and studies on documents (Table 4). After conducting interviews, observations and studies of institutional documentation, there was evidence and several findings in the Data and Information Center of X Government Institution. The next step was to do gap analysis by comparing the facts with ISO/IEC 27001:2013, which then poured them into work paper gap analysis, contained the conditions, causes, impacts, gaps, recommendations and objective control values as shown in Table 5. Work Paper Gap Analysis has 114 objective controls from ISO/IEC 27001:2013 that must be implemented by Data and Information Center. Of the 114 objective controls, Data and Information Center only applied 64 objective controls or the application of ISO/IEC 27001:2013 was 56.14% while the objective controls of ISO/IEC 27001:2013 that were not implemented by Data and Information Center were as many as 50 controls or 43.86%.

The next analysis phase was the maturity level analysis of each answers of assessment questions. Assessment was carried out for each control with assessment criteria ranging from 0 to 5. After an assessment had been carried out for each objective control, to get the final index of maturity level in each annex, the maturity level index of each objective control was averaged, so that a final index of maturity level for information security was obtained in the Data and Information Center of X Government Institution. Table 6 is the results of the maturity level assessment of each ISO/IEC 27001:2013 clauses on information security implemented by the X Government Institution.

The results of the final assessment of maturity level could illustrate the extent to which Data and Information Center had implemented information security based on ISO/IEC 27001:2013. The results of the assessment will be described and analyzed with a graph of maturity level modeling.

This analysis was conducted to determine the maturity level position of Data and Information Center of X Government Institution in implementing information security based on ISO/IEC 27001:2013. What would then be compared between the current institutional maturity level, the institution's standard maturity level in general, and the targeted maturity level or what X Government Institution wanted to achieve. Institutions generally had information security with level 3 of maturity level. While the Data and Information Center of X Government Institution wanted to achieve maturity level at level 4.

The modeling graph of maturity level will show the gap between the institution's maturity level position now and the standards of regulations, and the targets to be achieved. Figure 1 shows that the level of information security applied by Data and Information Center X Government Institution is level 1 namely Initial which means that there is evidence that the institution was aware of problems that must be addressed. However, there was no standard process, but used an ad hoc approach that tended to be treated individually or on a case-by-case basis. In general, the process approach was not organized.

The maturity level of institutions in general is at level 3. The information security applied by Data and Information Center of X Government Institution was still far below the information security of other institutions. The target to be achieved by Data and Information Center was information security with maturity level at level 4 or managed but based on the results of the maturity level analysis, Data and Information Center has not reached its desired target. Information security conditions owned by X Government Institution still have to be developed with reference to ISO/IEC 27001:2013 standards, such as adding some documentation and making improvements in implementing the control objectives contained in ISO/IEC 27001: 2013.

Figure 2 explains the results of the maturity level of each annex obtained which is then compared to the standard maturity level of ISO/IEC 27001:2013 (level 5) and the maturity level that is expected and targeted by X Government Institution (level 4). From the graph, there are several explanations, namely: (a) Information security of X Government Institution regarding Information Security Policy is at level 1 (Initial). This shows that there is evidence that the institution was aware of problems that must be addressed. In general, the process approach was not organized. (b) Information security of X Government Institution regarding Information Security Organization is at level 1 (Initial). This shows that there is evidence that institution was aware of problems that must be addressed. In general, the process approach was not organized. (c) Information security of X Government Institution regarding Human Resource Security is at level 3 (Defined). This shows that the procedures are standardized and documented and then communicated through training. Then it was mandated that these processes must be followed. However, irregularities could not be detected. The procedure itself was incomplete but had formalized current practices. (d) Information security of X Government Institution regarding Asset Management is at level 1 (Initial). This

shows that there is evidence that institution was aware of problems that must be addressed. In general, the process approach was not organized. (e) Information security of X Government Institution regarding Access Control is at level 2 (Repeatable). This shows that the process was developed into stages where similar procedures were followed by different parties for the same work. There was no formal training/communication of procedures, standards, and responsibilities submitted to each individual. There was a high level of trust in the individual to allow for very large errors. (f) Information security of X Government Institution regarding Cryptography is at level 1 (Initial). This shows that there is evidence that institution was aware of problems that must be addressed. In general, the process approach was not organized. (g) Information security of X Government Institution regarding Physical and Environmental Security is at level 1 (Initial). This shows that there is evidence that institution was aware of problems that must be addressed. In general, the process approach was not organized. (h) Information security of X Government Institution regarding Operation Security is at level 1 (Initial). This shows that there is evidence that institution was aware of problems that must be addressed. However, there was no standard process, but used an ad hoc approach that tended to be treated individually/per case. In general, the process approach was not organized. (i) Information security of X Government Institution regarding Communication Security is at level 2 (Repeatable). This shows that the process was developed into stages where similar procedures were followed by different parties for the same work. There was no formal training/communication of procedures, standards, and responsibilities submitted to each individual. There was a high level of trust in the individual to allow for very large errors. (j) Information security of X Government Institution regarding System Acquisition, Development and Maintenance is at level 2 (Repeatable). This shows that the process was developed into stages where similar procedures were followed by different parties for the same work. There was no formal training/communication of procedures, standards, and responsibilities submitted to each individual. There was a high level of trust in the individual to allow for very large errors. (k) Information security of X Government Institution regarding Supplier Relations is at level 1 (Initial). This shows that there is evidence that institution was aware of problems that must be addressed. In general, the process approach was not organized. (l) Information security of X Government Institution regarding Information Security Incident Management is at level 1 (Initial). This shows that there is evidence that institution was aware of problems that must be addressed. In general, the process approach was not organized. (m) Information security of X Government Institution regarding Information Security Aspects of Business Continuity Management is at level 1 (Initial). This shows that there is evidence that institution was aware of problems that must be addressed. In general, the process approach was not organized. (n) Information security of X Government Institution regarding Conformity is at level 1 (Initial). This shows that there is evidence that institution was aware of problems that must be addressed. In general, the process approach was not organized.

CONCLUSION

Based on the results and discussion, the following conclusions can be drawn: (1) Information security implemented by Government Institutions X is not in accordance with ISO/IEC 27001: 2013 standards. Of the 114 objective controls, only applied 64 or 56.14%. (2) Maturity levels and gaps in the information security of X Government Institution, it is concluded that the smallest annex values is Information Security Policy, Information Security Organization, Asset Management, Cryptography, Physical and Environmental Safety, Operation Security, Supplier Relations, Information Security Incident Management, Information Security Aspect of Business Continuity Management, and Conformity while the largest annex value is Human Resource Security.

REFERENCES

Abu Saad, B., Saeed, F.A., Alghathbar, K. and Khan, B., 2011. Implementation of ISO 27001 in Saudi Arabia–obstacles, motivations, outcomes, and lessons learned.

Al-Mayahi dan Mansoor. 2012. ISO 27001 Gap Analysis - Case Study.

Badan Standardisasi Nasional. 2016. Teknologi informasi – Teknik Keamanan –Sistem Manajemen Keamanan Informasi –Persyaratan. Jakarta: BSN.

Beckers, K., Côté, I., Faßbender, S., Heisel, M. and Hofbauer, S., 2013. A pattern-based method for establishing a cloud-specific information security management system. Requirements Engineering, 18(4), pp.343-395.

Beckers, K., Faßbender, S., Heisel, M., Küster, J.C. and Schmidt, H., 2012, February. Supporting the development and documentation of ISO 27001 information security management systems through security requirements engineering approaches. In International Symposium on Engineering Secure Software and Systems (pp. 14-21). Springer, Berlin, Heidelberg.

Candiwan, Candiwan & Y D Beninda, M & Priyadi, Yudi. 2016. Analysis of Information Security Audit Using ISO 27001:2013 & ISO 27002:2013 at IT Division -X Company, In Bandung, Indonesia. 10.13140/RG.2.1.1483.3044.

Chazar, Chalifa. 2015. *Standar Manajemen Keamanan*

Sistem Informasi Berbasis ISO/IEC 27001:2005 – Jurnal Informasi, Vol. 07, No. 2, November 2015: 48-57.

Cyber Security Breaches 2016. Laporan Cyber Security Breaches. United Kingdom: Department for Culture, Media & Sport.

Dewi, A.C., Nugroho, E. and Hartanto, R., 2017. *Manfaat Perealisasian Tata Kelola Keamanan Informasi Berbasis Sni Iso/iec 27001: 2009 pada Produksi Film Animasi (Kasus di PT. XX). Prosiding SNATIF, pp.843-847.*

Disterer, Georg. 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management – Journal of Information Security.

Expert Consultant Information System 2017. *Laporan Asesmen SNI ISO 27001. Jakarta.*

Hu, Q., Dinev, T., Hart, P. and Cooke, D., 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), pp.615-660.

IDCERT. 2013. *Profil Indonesia* Computer Emergency Response Team [online]. Available: *http://www.cert.or.id/tentang-kami/id/ [20 September 2017].*

Islami, D.C., IH, K.B. and Candiwan, C., 2016. Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia. INKOM Journal, 10(1), pp.19-26.

Jawadekar, W.S. 2002. Information system management. New Delhi: Tata McGraw-Hill.

Kementerian Komunikasi dan Informatika. 2016. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi. Jakarta: Kominfo.

Kementerian Komunikasi dan Informatika. 2012. Indeks Keamanan Informasi (KAMI) Versi 2.2. Jakarta: Kominfo.

Komalasari *dan* Perdana. 2014. *Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO/IEC 27001:2013: 2009 – Jurnal Sistem Informasi, Vol. 9 No. 2, September 2014: 201 – 216.*

Luo, X., Brody, R., Seazzu, A. and Burd, S., 2011. Social engineering: The neglected human factor for information security management. Information Resources Management Journal (IRMJ), 24(3), pp.1-8.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T., 2015. Information security conscious care behaviour formation in organizations. Computers & Security, 53, pp.65-78.

Sarno, Riyanarto *dan* Iffano, Irsyat. 2009. *Sistem Manajemen Keamanan Informasi. Surabaya: ITSPress.*

Surya dan Sulistyono. 2016. *Penilaian Keamanan Jaringan Menggunakan Standar ISO/IEC 27001 Pada Kantor Redaksi Harian Suara Merdeka - Journal of Information System.*

Susanto12, H., Almunawar, M.N. and Tuan, Y.C., 2011. Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECSIJENS, 11(5), pp.23-29.

Tu dan Yuan. 2014. Critical Success Factors Analysis on Effective Information Security Management: A Literature Review - Twentieth Americas Conference on Information Systems, Savannah, 2014

Whitman dan Mattord. 2014. Management of Information Security. Stamford: Cengage Learning.

APPENDIX

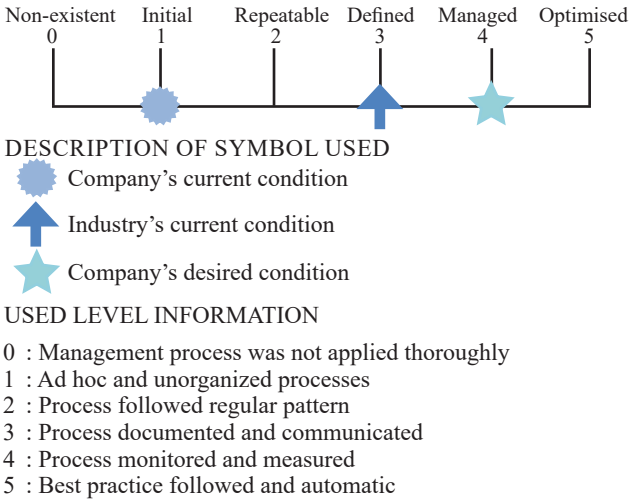

Figure 1. Overall Analysis Graph of Maturity Level

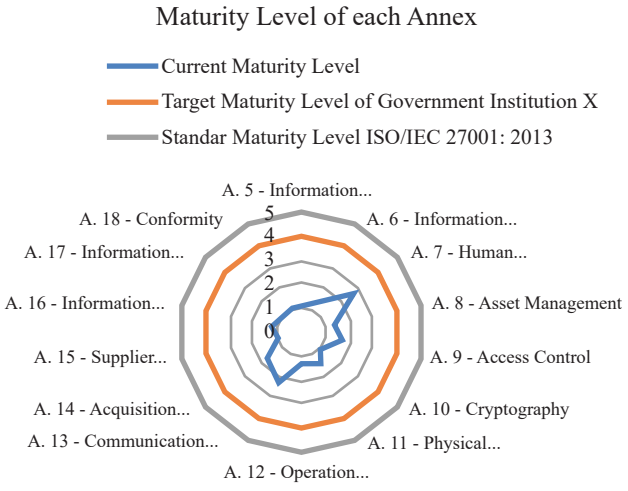

Figure 2. Graphic of Maturity Level of Each Annex

Table 1. Maturity Levels and Their Definition

Maturity Level	Definition
0 - Non- Existent	A complete lack of any recognizable process. The institution does not even know that there are problems that must be addressed.
1 – Initial	There is evidence that institutions are aware of problems that must be addressed. However, there is no standard process, but uses an ad hoc approach that tends to be treated individually/per case. In general, the process approach is not organized.
2 – Repeatable	The process is developed into stages where similar procedures are followed by different parties for the same work. There is no formal training/ communication of procedures, standards, and responsibilities submitted to each individual. There is a high level of trust in the individual to allow for very large errors.
3 – Defined	Procedures are standardized and documented and then communicated through training. Then it is mandated that these processes must be followed. However, irregularities cannot be detected. The procedure itself is incomplete but has formalized current practices.
4 – Managed	Management monitors and measures compliance with procedures and takes action if the process cannot be done effectively. The process is under constant increase and the good practice provision. Automation and devices are used within certain limits.
5 – Optimized	The process has been selected into a good level of practice, based on the results of continuous improvement and modeling of maturity with other institutions. Information technology is used as an integrated way to automate workflows, providing tools to improve quality and effectiveness and make institutions adapt quickly.

Table 2. Maturity Indexes and Maturity Levels

Maturity Index	Maturity Level
0– 0,49	0 - Non-Existent
0,50 – 1,49	1 – Initial
1,5 - 2,49	2 – Repeatable
2,5 – 3,49	3 – Defined
3,5 – 4,49	4 – Managed
4,5 – 5,00	5 – Optimized

Table 4. Summary of Assessment Result

Annex	Summary
A.5 - Information Security Policy	Policies that have been made by the Data and Information Center such as the ICT Information Security Policy, Project Management Policy, Standard Policy for the Management of ICT Services, Project Management SOPs and other policies and SOPs that have not yet been fully implemented. These policies have never been reviewed.
A.6 - Information Security Organization	Data and Information Center has not defined the roles and responsibilities of information security for personnel from third parties, apprentices, etc. which are directly related to access to data and data processing systems. Efforts to separate tasks have been carried out but do not have a policy. Data and Information Center always maintains contacts of various institutions related to security, technology, law and so on. Data and Information Center has not specifically adopted information security aspects in project management activities. Data and Information Center does not have a specific policy to deal with risks that occur due to the use of mobile devices. X Government Institution does not carry out teleworking in its activities.
A.7 - Human Resource Security	Data and Information Center does not have a formal policy related to information classification and risk analysis of each information. X Government Institution has implemented written agreements regarding the obligations of employees and contractors using NDA. There is no formal policy related to the information security management system that can be used as a reference for carrying out duties and responsibilities related to employee development in terms of information security. The disciplinary process has been carried out in accordance with staffing provisions that apply to civil servants but has not been specifically applied. Dismissal mechanisms and changes in staffing in Government Institutions X have followed staffing regulations but have not been equipped with formal procedures.
A.8 - Asset Management	X Government Institution has been able to identify all assets related to information processing, but there are no guidelines for inventorying specific assets related to information assets. Assignment of assets to employees has been carried out using handover letters but there is no mechanism and documentation of assets when the assets are returned. There are no procedures governing the management of removeable storage media.
A.9 - Access control	Data and Information Center has carried out various access controls such as the use of access cards to enter the area of buildings and rooms that are within the X Government Institution

	and Data and Information Center, the placement of security officers to manage access and exit from external parties and the use of passwords to access systems and applications. Control and restrictions on physical access are not carried out in a disciplined manner. There is no formal policy regarding access control. Data and Information Center already has SOPs related to access to network services such as services for creating email accounts, opening internet access and opening user access rights. User ID is obtained through the registration process in advance, but the formal process related to registration is not owned by Data and Information Center.
A.10 - Cryptography	Data and Information Center has used cryptographic techniques in order to protect information, but the use is still ad hoc, and no risk analysis has been carried out to determine analytical techniques. The existing cryptographic keys are generally still associated with a single key such as a password. Protection of cryptographic keys is still carried out in an ad hoc manner and is not well organized. Data and Information Center does not have a policy regarding cryptography.
A.11 - Physical and Environmental Safety	In general, personnel who can enter the room at the office of X Government Institution have been filtered. Data and information security, especially in the server room, is still relatively low. There is no definitive special treatment for the security of server and archive rooms. In every room X Government Institution has installed an RFID-based access control device and its use procedures are applied. Only authorized personnel (having X Government Institution employee cards) can enter the room. In each room, an access control device has been installed to prevent unauthorized access and has a raised floor installed in the server room to reduce the risk of disaster, but there is no specific guide to equipment placement.
A.12 - Operation Security	Information processing is carried out based on needs or requests. X Government Institution does not yet have operational procedures for managing information including the process of request, processing and transfer or deletion. The information processing process is currently running even without procedures. Malware control currently uses NOD anti-virus. Backup information has been done regularly and backup testing has been done but there is no policy regarding information backup.
A.13 - Communication Security	The network has been managed even though it is not routine. The tasks and functions of network management are not performed properly and correctly. Network evaluation is not done regularly. There are no regulations governing electronic messages. Lack of understanding of risk and confidentiality of information. The NDA process has been carried out to third parties.
A.14 - System Acquisition, Development and Maintenance	No information security requirements and control documents were found in the system or application development document. There is already control over the use of information networks to the public. There are no regulations regarding information protection from outside or unauthorized access. The principle for system engineering has been carried out only not yet well documented. Data and Information Center already has a different development environment than production. Data and Information Center has already supervised the system development carried out by outsiders. Acceptance testing and its criteria have been arranged and prepared both for the new system but not yet documented.
A.15 - Supplier Relations	At present there is no information security policy associated with cooperation with third parties, the agreement is still based on KAK. Lack of knowledge about risks to the impact of services by third parties. There is no agreement with suppliers regarding the information security risk requirements for services and products.
A.16 - Information Security Incident Management	There is no system for assessing the duties and responsibilities for information security incidents. There is currently no formal and periodic reporting on information security events. Reports are ad hoc according to the events that occur. Information security incidents were responded to but did not follow procedures because there were no procedures for handling information security incidents.
A.17 - Information Security Aspect of Business Continuity Management	There is no document regarding business continuity related to information security. There is no document to maintain the security of information security. Lack of employee knowledge in building information security aspects of business continuity management. A backup process is found but only for certain systems and does not use real time for the main application.
A.18 - Conformity	At present the X Government Institution is applying the Minister of Communication and Information Regulation about the ISMS and other regulations related to information or data security. Copyright procedures have not been found. Protection of personal information has not been done thoroughly and systematically, it is still ad hoc or based on situations and events. A plan for periodic assessment of information security has not been found.

Table 3. Maturity Level Assessment

ANNEX							
ANNEX	**Control**	**Question**	**Yes**	**No**	**index / objective control value**	**index / control average**	**average of clause value & maturity level**
5	**INFORMATION SECURITY POLICY**						
5.1	**MANAGEMENT DIRECTION FOR INFORMATION SECURITY**						
	OBJECTIVE to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.						
5.1.1	POLICY FOR INFORMATION SECURITY	Is there policy for information security established, approved by management, issued and communicated to employees and related external parties?	√		1	1	**1 Initial**
5.1.2	INFORMATION SECURITY POLICY REVIEW	Is there policy for information security that has been reviewed in a planned time interval?	√		1		

Table 5. Work Paper Gap Analysis

ANNEX	CONTROL	CONDITION	EVALUATION	RECOMMENDATION	OBJECTIVE CONTROL VALUE
5	**INFORMATION SECURITY POLICY**				
5.1	**MANAGEMENT DIRECTION FOR INFORMATION SECURITY**				
	OBJECTIVE to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.				
5.1.1	**POLICY FOR INFORMATION SECURITY CONTROL** a set of policies for information security must be established, approved and communicated to employees and related external parties.	**CONDITION** Data and Information Center used to design ICT information security policies, following were some of policy and procedure documents, which had referred to ISO 27001. The policies that had been designed among others were: • ISMS Policy & Standards • Project Management Policy • SDLC Policy • ICT Service Management Standard Policies • Project Management SOP • And others **CAUSE** • The developed information security policies design was not formally established, approved by the management, published and communicated to employees and related external parties. • The information security policies design was still incomplete as required by ISO 27001.	**GAP** According to Annex 5, objective control 5.1.1, policies that had been made should be communicated to the employees and related external parties, so the policies can be established. **IMPACT** • The efforts made to perform information security still an ad hoc, not structured and reactive too, which cause the objective of information security yet to be achieved effectively, efficiently, and optimally. • The efforts for certification of ISMS needed basic correction.	**RECOMMENDATION** Data and information Center needed to define a higher level of "Information Security Policy" in accordance to ISO 27001 and ISO 27002, then approved by top management, which described the organization approach in managing information security's objectives, and also communicated to employees and related external parties.	1

Table 6. Maturity Level per Clause

Clause	Level	
A.5 - Information Security Policy	1	Initial
A.6 - Information Security Organization	1,4	Initial
A.7 - Human Resource Security	2,6667	Defined
A.8 - Asset Management	1,2777	Initial
A.9 - Access control	1,5667	Repeatable
A.10 - Cryptography	1	Initial
A.11 - Physical and Environmental Safety	1,4722	Initial
A.12 - Operation Security	1,2857	Initial
A.13 - Communication Security	2,25	Repeatable
A.14 - System Acquisition, Development and Maintenance	1,7407	Repeatable
A.15 - Supplier Relations	1	Initial
A.16 - Information Security Incident Management	1,2875	Initial
A.17 - Information Security Aspect of Business Continuity Management	1	Initial
A.18 - Conformity	1,1	Initial
Average	1,432	Initial