International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Analysis of System Security Levels of Tax Payment and Regional Retribution Based on ISO / IEC27002: 2013 Standard Using SSE-CCM

Aburizal Rosadi[1], Bheta Agus Wardijono[2]
[1]Business Information System, Gunadarma University, Depok, West Java – Indonesian-16424
[2]Computer Science, STMIK Jakarta STI&K, South Jakarta, Jakarta – Indonesian-12140

Abstract— *An online system for paying local taxes and levies was built to speed up the tax payment process as well as to monitor tax payments. The system being developed must have a good level of security due to the large amount of data and transactions related to finance, so it is very dangerous if the system cannot protect data properly. Security analysis needs to be done to ensure the system can protect data properly, so the security analysis refers to the ISO 27002: 2013 standard by establishing clause 9 of access control, clause 10 of cryptography, clause 12 of operational security and clause 16 of information incident management. The access contract has a security level of 4.42, cryptography has a security level of 3, operational security has a security level of 5 and information security management has a security level of 3. It can be concluded that the system security level in the clause that has been set is 3.85 which means the security level is at level 4 or Managed and Measurable.*

Keywords— *ISO 27002:2013, SSE-CMM, System Information, nformation System Security.*

I. INTRODUCTION

Data security is very important in maintaining the confidentiality of information, especially if it contains sensitive information, which only authorized parties can know, especially if the data is transmitted over the internet. In the online system for paying local taxes and levies, there are many sensitive data transactions ranging from data on taxpayers or customers, data from regional tax recipient bodies, data from the bank as the party facilitating the banking system. If there is a wiretap or data is not properly secured, it will cause losses, especially from a financial perspective.

Basically, a secure system has the ability to protect the data in it, from a number of possible attacks, including:

1. *Instruction* in this method an attacker can use a computer system that is owned by someone else, some of this type of attack wants access as well as users who have the right to access the system.
2. *Denial of service* is an attack that causes the user to be unable to access the system because there is a bottleneck that occurs in the system.
3. SQL injection is an attack that allows unauthorized users to access the server database or enter SQL comments into SQL queries.
4. Key Loger is an activity to record computer user activity.
5. *Malware this* form of attack is software that has a high level of danger because the system contains a virus. Malware can quickly damage what's on the system, from destroying information systems to stealing important data.
6. *Phishing* attacks are related to data theft

An online tax and levy payment system was built to speed up the tax payment process as well as *monitor* tax payments. The system built consists of a customer system, a bank system, and an online tax payment system that communicates with one another.

The number of sensitive data communications from an integrated system requires the security of each system to ensure security in data communication. Based on information from data.jakarta.go.id in 2019, the number of taxpayers in DKI Jakarta was 13,664,874 taxpayers. With a large number of taxpayers and will be integrated with the system, there will also be a lot of integrated transaction data.

Security issues are a very important aspect of an information system, where an intruder is able to enter the system and commit data theft or perform other harmful actions. So far, the online tax payment system developed by PT XYZ has never been analyzed regarding the security aspects of the system and PT XYZ has not yet known to what extent the security level of the online tax payment system being developed. Therefore, it is necessary to analyze the security of the tax payment system aimed at maintaining the confidentiality, integrity and availability aspects of the information.

II. THEORITICAL BASIC

A. *Information System*

In general, an information system is a system that exists in an organization in which there is a combination consisting of a collection of people, facilities, technology and even ways of working or methods so as to create a flow of communication and processing of various types of internal and external events that can be used as a basis. in making decisions based on the information contained in the system.

A system cannot run without support or operation and management support which includes a combination of information technology and various human activities who act as users of the technology itself.

An equation that stands out is that an information system combines various kinds of data collected from various sources to be able to combine data from various sources in a data *transformation* system so that it is *compatible*. Regardless of

Aburizal Rosadi and Bheta Agus Wardijono, "Analysis of system security levels of tax payment and regional retribution based on ISO / IEC27002: 2013 standard using SSE-CMM," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 1, pp. 205-211, 2021.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

its size and scope, an information system needs to be *compatible* (*compatibility*).

B. *Information Security*

Information security describes efforts to protect computers and non-computer equipment, facilities, data and information from misuse by irresponsible people. This definition includes quoters, fax machines, and all types of media, including paper documents and smartphones. For smartphone use, communication has become a daily necessity. From several cases, the use of smartphones can be misused for computer crimes, from fraud to extortion. (Kohar, Abdul, et al., 2015).

Information security aspects include three things, namely: Confidentiality, Integrity, and Availability (CIA). These aspects are described as follows:

1. *Confidentiality*
   Aspects that ensure the confidentiality of information or data and ensure that information can only be accessed by authorized parties.
2. *Integrity*
   Aspects that guarantee data cannot be changed without the permission of the authorities, maintain the completeness of the information and protect it from damage or other threats that can cause changes to the original information or data.
3. *Availability*
   Aspects that ensure that data will be available when needed and ensure that users can access information without interruption.

According to (Whitman & Mattord, 2011) information is an important asset to protect its security. Companies need to pay attention to the security of their information assets, information leakage and system failures can result in losses both on the financial side and the company's productivity. Security in general can be defined as '*quality or state of being secure-to be free from danger*

C. *Information System Security Standards*

According to ISO / IEC 27000: 2014, ISMS is a systematic approach to establish, implement, operate, monitor, review, maintain and improve information security in organizations to achieve business goals. According to ISO / IEC 27001: 2014, information system security is not only related to the use of antivirus software, firewalls, the use of passwords for computers, but an overall approach from the perspective of people, processes and technology to ensure the effectiveness of security.

ISO is an international standard body consisting of representatives and national standardization bodies of each country established on February 23, 1947, ISO sets world industrial and commercial standards. In establishing an ISO standard, inviting representatives of its members in a technical committee (TC), sub committee (SC) and working group (WG). ISO works closely with the international electronics commission (IEC) which is responsible for the standardization of electronic equipment.

ISO 27000 was published in 2009 to provide an overview of the ISO 27000 standard as well as its conceptual basis in general. There are 46 basic information security defined in "*Terms and Conditions*" ISO 27000. Information security is based on companies whose business processes depend on IT infrastructure that is prone to failures and disruptions. As with other information technology standards, ISO 27000 refers to the cycle PDCA *(Plan - Do - Check - Action)*, a well-known cycle of quality management.

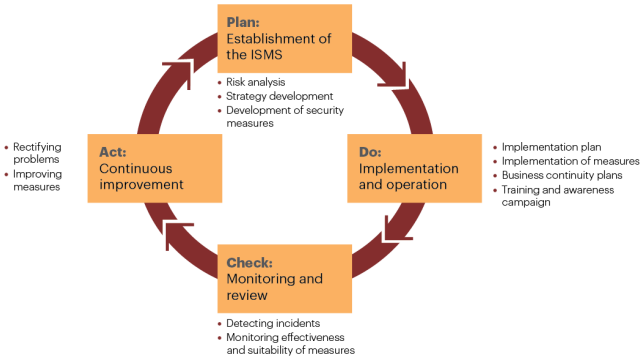

Fig. 1. PDCA Cycle ISO 27001

III. RESEARCH METHOD

A. *SSE-CMM Method*

SSE-CMM (*System Security Engineering - Capability Maturity Model*) is a calculation model used to measure security levels, develop processes such as engineering processes and non-technical processes. SSE-CMM consists of two parts, namely:

1. Models for process, project and organizational security engineering.
2. Assessment method to determine the level of process security

The SSE-CMM model provides a comprehensive overview of the principles and architecture based on SSE-CMM, an executive overview of the model, suggestions for appropriate model use, practices included in the model, and description of the attributes of the model. The SSE-CMM assessment method describes processes and tools for evaluating an organization's security engineering capabilities.

To identify and assess the ability of the organization whether it has met good information security standards, an identification framework can be used which is represented in a maturity level that has a grouping level of company capabilities, as described in table 1.

TABLE 1. Kirteria security level assessment index

Level	Range	Information
0	0 – 0.50	*Non-Existent*
1	0.51 – 1.50	*Initial / Ad Hoc*
2	1.51 – 2.50	*Repeatable But Invinitve*
3	2.51 – 3.50	*Define Process*
4	3.51 – 4.50	*Managed and Measurable*
5	4.51 – 5.00	*Optimized*

As described in table 1, the SSE-CMM method has five levels of ability to indicate the process level. A description of the level of assessment for the SSE-CMM method is described in Table 2.

Aburizal Rosadi and Bheta Agus Wardijono, "Analysis of system security levels of tax payment and regional retribution based on ISO / IEC27002: 2013 standard using SSE-CMM," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 1, pp. 205-211, 2021.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

TABLE 2. Kirteria level security level

Level	Information
0	not all basic practice is carried out
1	all basic practices are carried out but in an informal manner, which means there is no documentation, no standard and is carried out separately.
2	planned and tracked which indicates a commitment to planning the standard process.
3	well defined, which means the standard process has run according to the definition
4	controlled quantitatively, which means quality improvement through monitoring each process.
5	constantly being improved which means the standard has been perfect and a focus on adapting to change.

B. *ISO 27002*

ISO / IEC 27002 was developed to provide guidance on implementing information security. ISO / IEC 27002 is widely used in overcoming problems related to information security (Gehrmann, 2012). ISO 27002 is able to provide guidance in planning and implementing programs to protect information assets (Rahman, 2016). Which, if linked to ITIL, can help create a process related to IT delivery and support (Simonsson and Johnson, 2008).

ISO / IEC 27002 provides sound information security management recommendations. Where information is an important object in business processes in organizations. Standards and procedures related to information security and control enable organizations to apply good security to their information. ISO / IEC 27002 not only secures IT-based information, but information stored in physical form such as paper is a concern in its use.

C. *Data Collection Technique*

The data used in this research is divided into two, namely primary data which is the main research data and secondary data as supporting data in this research.

Primary data which is the main data obtained from:

1. Observation, namely observing in the field the application and use of online systems for paying local taxes and levies.
2. Interviews, giving direct questions to sources who are also respondents.

Controls are designed to ensure that actions can ensure that organizational goals are achieved and unwanted events are prevented, detected and corrected.

In distributing the questionnaire, the authors made a list of questions based on the standards contained in ISO 27002/17799 / BS 7799 regarding the guidelines for implementing information security management which consisted of 13 objective controls and 43 security controls spread out in 3 clauses. Secondary data that the writer uses in this research is obtained through literature or literature studies such as books, journals, proceedings and pages. From the results of distributing questionnaires then processed.

In this study there were 6 respondents. The scale used in this questionnaire uses the Guttman scale. With this type of measurement scale, you will get a firm answer, namely yes-no, true-false, never-never, positive-negative, and so on.

D. *System Design*

The online system for paying local taxes and levies is an access to reporting, monitoring, and paying local taxes and levies online. This system is one of the public services for taxpayers and Bapenda to improve their performance and facilitate payment transactions and tax reporting. The online system for paying local taxes and levies has the same components as other systems. These components are hardware, software, data, procedures, and people.

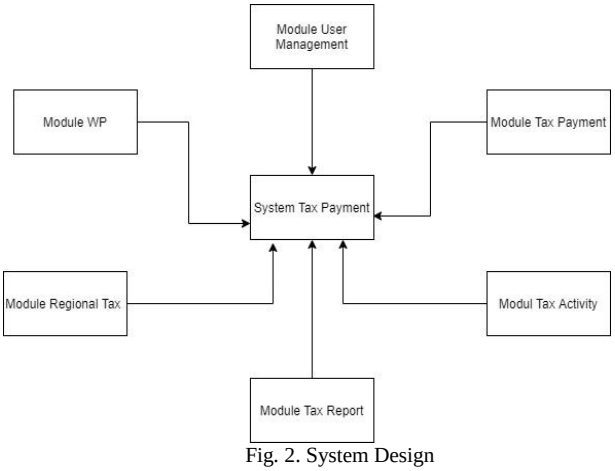

Fig. 2. System Design

E. *Systems Architecture*

The online system for paying local taxes and levies consists of several systems, including systems owned by taxpayers, tax payment web systems, bank systems, and tax reporting systems to systems owned by bapenda. Between the taxpayer system and the tax payment web system, there is an *engine* or application for *mapping data* in the taxpayer database to retrieve data as a basis for tax calculation, the system is integrated with the bank system as a payment service with API, the online tax web system will send *requests* to make a payment then the bank system will send a *response* to the *request* sent, the online tax web system is also integrated with the bapenda system for tax reporting using the API, the tax online web system will send *requests* for tax reporting and the bapenda system will send *responses* to *requests* sent.

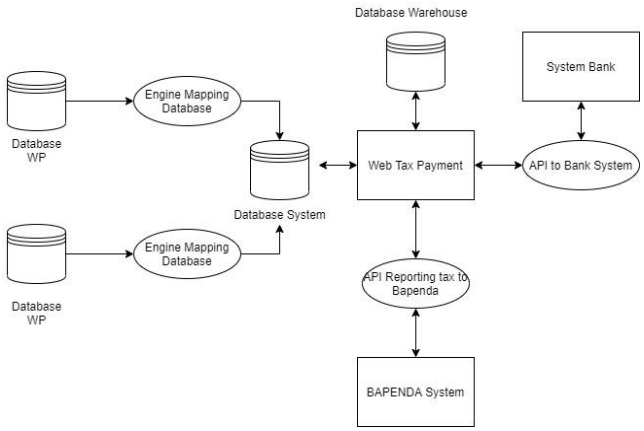

Fig. 3. Systems Architecture

Aburizal Rosadi and Bheta Agus Wardijono, "Analysis of system security levels of tax payment and regional retribution based on ISO / IEC27002: 2013 standard using SSE-CMM," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 1, pp. 205-211, 2021.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

IV. RESULT

A. Clause ISO 27002:2013

After making observations, the results obtained were the stipulation of the information system security clause from the standard used was ISO 27002: 2013. From this identification stage, the determination of clauses, control objectives, and security controls will be generated.

The clauses used in this research are clause 9 about access control, callus 10 about cryptography, clause 12 about operational security and callusul 16 Information security incident management.

B. *Maturity Level*

1. *Maturity Level Klausul 9*

Result of the maturity level calculation process in clause 9 regarding access control is 4.42. There are several aspects that need to be considered in the system, namely the allocation of secret authentication information controlled through a formal management process, and periodic review of user access rights that have not been applied to the system.

The results of calculating the maturity level in clause 9 regarding access control can be seen in table 4 and in graphical form in fig. 4.

TABLE 4. Maturity Level Klausul 9

Clause	Control Objectives	Security Control	Ability Level	Average Control Objectives
9 Access control	9.1 Business requirements for access control	9.1.1 Access control policy	5	5
		9.1.2 Network Access and Network Services	5	
	9.2 User access management	9.2.1 User registration and cancellation of user registration	3.3	2.66
		9.2.2 User Access Provider	5	
		9.2.3 Processing of privileged access rights	5	
		9.2.4 Management of user confidential authentication information	0	
		9.2.5 Review of user access rights	0	
	9.3 User responsibility	9.3.1 Use of confidential authentication information	5	5
	9.4 Access control systems and applications	9.4.1 Restrictions on access to information	5	5
		9.4.2 Secure log-on procedures	5	
		9.4.3 Password management system	5	
		9.4.5 Access Control to Source Code	5	
Average				4.42

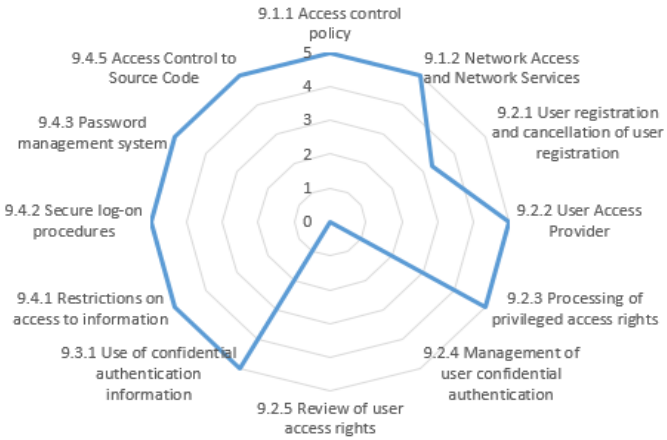

Fig. 4. Maturity Level Clause 9

2. *Maturity Level Klausul 10*

The result of the Maturity level 10 cryptographic process is 3.0. the system has implemented encryption in several parts, namely the API from and to the bank system is encrypted with ISO 8583 according to banking standards, the source code or application is encrypted and compiled securely, but there are some parts of the system that have not implemented encryption in data exchange between APIs, namely API to BAPENDA for reporting has not applied encryption to data exchange, and the application of mapping taxpayer data to system databases has not applied data encryption.

The results of level 10 maturity calculations can be seen in table 5 and in graphical form in fig. 5.

TABLE 5. Maturity Level Klausul 10

Clause	Control Objectives	Security Control	Ability Level	Average Control Objectives
10. Cryptography	10.1 Cryptographic controls	10.1.1 Policy on the use of Cryptographic controls	3	3
Average				3

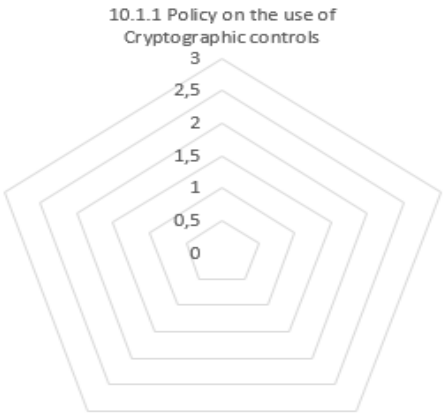

Fig. 5. Maturity Level Clause 10

3. *Maturity Level Klausul 12*

The result of the Maturity level 12 cryptographic process is 5.0, this indicates that in clause 12 the system is optimal, the system has implemented:

Aburizal Rosadi and Bheta Agus Wardijono, "Analysis of system security levels of tax payment and regional retribution based on ISO / IEC27002: 2013 standard using SSE-CMM," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 1, pp. 205-211, 2021.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

a. Control changes to organizations, business processes, information processing facilities and systems that affect information security
b. Operational activities in system development are well documented
c. Detection, prevention and recovery controls are implemented to protect against malware.
d. There are backup copies of information, software and system images retrieved and regularly tested according to agreed backup policies
e. Event logs that record user activity, exceptions, errors, and information security events are stored, and reviewed periodically
f. Loging facilities are protected and log information is protected from interference and unauthorized access
g. Information about the technical vulnerabilities of the information systems in use is obtained in a timely manner, the organization's exposure to these vulnerabilities is evaluated and appropriate action is taken to address the associated risks.

TABLE 6. Maturity Level Clause 12

Clause	Control Objectives	Security Control	Ability Level	Average Control Objectives
12. Operation safety	12.1 Operational procedure and responsibilities	12.1.1 Operational Documentation Procedure	5	5
		12.1.2 Change management	5	
	12.2 Protection from malware	12.2.1 Controls against malware	5	5
	12.3 Backup	12.3.1 Information backup	5	5
	12.4 Logging and monitoring	12.4.1 Event logging	5	5
		12.4.2 Protection of log information	5	
	12.6 Technical vulnerability management	12.6.1 Management of technical weakness	5	5
Average				5

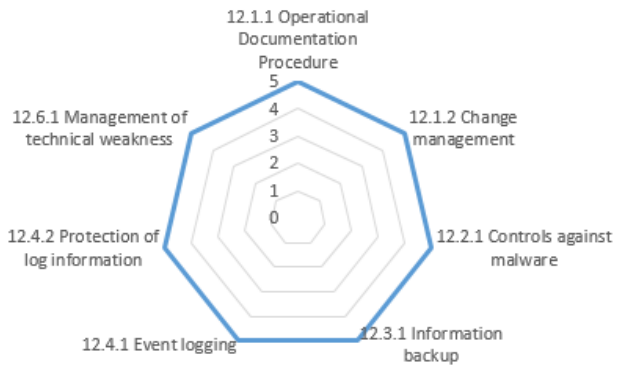

Fig. 6. Maturity Level Klausul 12

4. *Maturity Level Klausul 16*

The result of the Maturity level process clause 16 incident management and information system security is 3.0. The system has implemented:

a. Management responsibilities and procedures are in place to ensure prompt, effective and orderly response to information security incidents
b. Information security incidents are reported through the appropriate management channels as quickly as possible
c. Employees and users who use the organization's information systems and services have been asked to record and report any information security weaknesses observed or suspected in the system or service.

System has not documented and classified information system security incidents, and information incident handling has not been in accordance with formal documentation.

TABLE 7. Maturity Level Clause 16

Clause	Control Objectives	Security Control	Ability Level	Average Control Objectives
16. Information security incident management	16.1 Incident management and information security enhancement	16.1.1 Responsibilities and procedures	5	3
		16.1.2 Report information security incidents	5	
		16.1.3 Report information security weaknesses	5	
		16.1.4 Assessments and decisions about information security incidents	0	
		16.1.5 Response to information security incidents	0	
Average				3

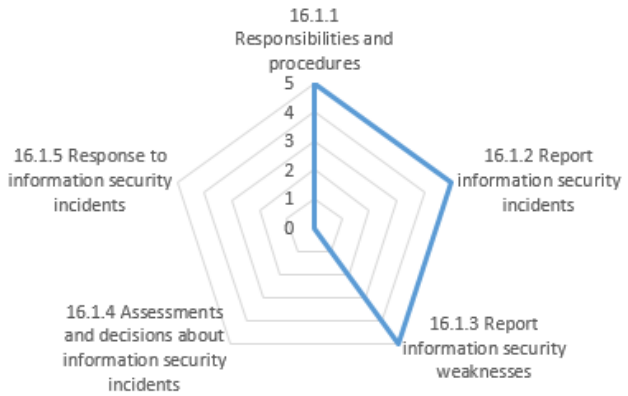

Fig. 7. Maturity Level Klausul 16

5. *Gap Analis*

Based on the calculation of the maturity level of the information system security from the online system for paying local taxes and fees, it is currently worth 3.85 and is included in level 4 and it is expected that the security level is 5

Aburizal Rosadi and Bheta Agus Wardijono, "Analysis of system security levels of tax payment and regional retribution based on ISO / IEC27002: 2013 standard using SSE-CMM," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 1, pp. 205-211, 2021.

(optimized). The calculation of the difference or gap for information system security analysts can be seen in table 8.

TABLE 8. Gap Analis

Clause	Information	Maturity Level		Gap
		Present condiition	Expected conditions	
9	Access Controls	4.42	5	0.58
10	Cryptography	3	5	2
12	Operation safety	5	5	0
16	Information security incident management	3	5	2
Average				1.145

Based on table 8, the value of the gap between the current condition and the expected condition for each clause is in clause 9 has a gap of 0.58, clause 10 is worth gap 2, clause 12 is gap 0, and clause 16 is gap 2

From these results then averaged to get the value of the gap or gap, then getting a value of 1.145 means that the gap value between the current condition and the expected condition still has a gap, so improvement is needed in each control. Recommendations will be given to each control so that the focus is on improving security controls, the ratio of the maturity level of the current condition to the conditions that are expected to be depicted in the graph in fig. 8.

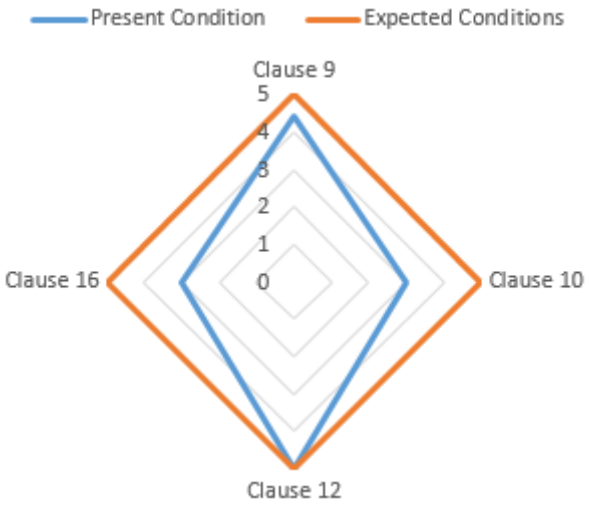

Fig. 8. Gap Analis

6. *Result*

Based on the calculation of maturity levels and analyst gaps in clauses 9 access control, 10 cryptography, 12 information security and 16. Information security incident management.

Clause 9 access control has a value of 4.42 and is at level 4 (*Managed and Measurable*). In clause 9 the system has categorized users and user access rights in accessing the system both databases, servers and applications, with user access control management only users who are given special access can directly access data in the database, application source code and application servers, lack of systems based on Clause 9 is the absence of periodic review of user access rights which if allowed by the user who is actually no longer allowed to access the database, application or server can still access using the old user's credentials and can cause problems in the future.

Clause 10 Cryptography has a value of 3 and is at level 3 (*Define Process*). The use of cryptography in the system has been applied to the API for data exchange to the bank system using ISO 8583 which is an international standard for banking transactions, the weakness of the system based on clause 10 is that cryptography has not been applied to API to bapenda and the data mapping system from taxpayers to the system database.

Clause 12 Information Security has a value of 5 and is at level 5 (*Optimized*), based on clause 12 the system has been declared optimal, the system can anticipate malware, implement application and database backups, the system can log user activity logs, and has operational procedures and responsibilities.

Clause 16 has a value of 3 and is at level 3 (*Define Process*). Based on clause 16, the system has implemented management responsibilities and procedures to ensure prompt, effective and orderly response to information security incidents, information security incidents have been reported through the appropriate management channels as quickly as possible, the system has not documented and classified information system security incidents, and information incident handling is not in accordance with formal documentation.

Overall the system average has a value of 3.85 and is at level 4 (*Managed and Measurable*).

V. CONCLUSION

Based on the results of data processing, the following conclusions can be drawn:

1. The application of the ISO 27002: 2013 standard in the online system for paying taxes and levies in the DKI Jakarta area is at level 4 which means it is controlled quantitatively, which means quality improvement through monitoring each process.
2. The system is analyzed based on ISO / IEC 27002: 2013 standards with clauses 9, 10, 12, and 16. Clause 12 has been declared optimal, while the system is still not declared optimal in clause 9 of access control, clause 10 on cryptography and clause 16 Information security incident management.
3. System communication using API to the bank system has been declared safe because it implements cryptography using the ISO 8583 standard, it's just that the API for exchanging data to the bapenda system and applications for data mapping from taxpayers to the system database has not implemented cryptography.
4. The system has implemented a database backup and registration of user permissions who can access the database and applications directly with different user permissions.

Aburizal Rosadi and Bheta Agus Wardijono, "Analysis of system security levels of tax payment and regional retribution based on ISO / IEC27002: 2013 standard using SSE-CMM," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 1, pp. 205-211, 2021.

REFERENCES

[1] Mahersmi, Balqis Lembah., Muqtadiroh, Feby Artowini., Hidayanto, Bekti Cahyo. 2016. "Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode Octave Dan Kontrol Iso 27001 Pada Dishubkominfo Kabupaten Tulungagung". Seminar Nasional Sistem Informasi Indonesia, 1 November 2016.

[2] Windirya, Danastri Rasmona., Tanuwijaya, Haryanto., Sutomo3,Erwin. 2013. "Audit Keamanan Sistem Informasi Pada Instalasi Sistem Informasi Manajemen Rsud Bangil Berdasarkan ISO 27002". JSIKA Vol 3, No 2 (2013)/ ISSN 2338-137X

[3] Purba, Altry David., Purnawan, I Ketut Adi., Pratama, I Putu Agus Eka. 2018. "Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5". MERPATI VOL. 6, NO. 3 DESEMBER 2018. ISSN: 2252-3006

[4] Kurniawan, Endang. 2018 "Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM". Tesis Universitas Islam Indonesia.

[5] Jeperson Hutahaean. (2014)."Konsep Sistem Informasi". Konsep Sistem Informasi (Vol. 53).

[6] Kohar, Abdul & Riadi, Imam & Lutfi, Ahmad. (2015). Analysis of Smartphone Users Awareness Activities Cybercrime. International Journal of Computer Applications. 129. 1-6. 10.5120/ijca2015906449.

[7] Febrianto, Ferry., Sensuse, Dana Indra. 2017 "Evaluasi Keamanan Informasi Menggunakan ISO/IEC 27002: Studi Kasus Pada Stimik Tunas Bangsa Banjarnegara" INFOKAM Nomor II Th. XIII/SEPTEMBER/2017.

[8] Syafitri, Wenni. 2016. "Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)". Jurnal CoreIT, Vol.2, No.2, Desember 2016. ISSN: 2460-738X (Cetak).

[9] Disterer, Georg. 2013. "ISO/IEC 27000, 27001 and 27002 for Information Security Management". Journal of Information Security, 2013, 4, 92-100

[10] INTERNATIONAL STANDARD ISO/IEC 27002. 2013 "Information technology — Security techniques — Code of practice for information security controls". Available at https://trofisecurity.com/assets/img/ISO-IEC_27002-.pdf.[Accessed , 21 November 2020]

[11] Jakarta Open Data (2020). Data Wajib Pajak Retribusi Daerah DKI Jakarta tahun 2019 [Online]. Available at: https:// data.jakarta.go.id, [Accessed 21 November 2020].

[12] Whitman, E Michael., Mattord J Horbert., (2011) "Roadmap To Information Security: For It And Infosec Managers".

[13] Kadir, A. (2009). "Pengenalan Sistem Informasi". American Enterprise Institute for Public Policy Research.

[14] Kristanto, A. (2007)."Pengertian sistem informasi. Pengertian Sistem Informasi",7.

[15] Jogiyanto. (2009)."Analisis dan Desain". Yogyakarta: Andi, 53, 160.