Available online at https://journal.rescollacomm.com/index.php/ijqrm/index

International Journal of Quantitative Research and Modeling

e-ISSN 2721-477X
p-ISSN 2722-5046

Vol. 4, No. 3, pp. 166-171, 2023

Information System Security Audit Sistem Informasi Kearsipan (SIMKA) at Badan Pendapatan Daerah Jawa Barat Kota Bandung III Using COBIT 5 Framework and Standard IS0/IEC 27002

Suci Fitriani Setiawan[1*], Titan Parama Yoga[2], Budiman[3]

[1,2,3]*Faculty of Technology and Informatics Universitas Informatika dan Bisnis Indonesia, Bandung, Indonesia*

**Corresponding author email: fitrianiveerbeck@gmail.com*

Abstract

One of the main problems for an agency or a company is the security of information systems. High security is needed to maintain the confidentiality and misuse of information within the organization. To improve the security of business operations and the quality of information technology resources, it is necessary to evaluate to op Badan Pendapatan Daerah Jawa Barat Kota Bandung III, namely SIMKA BAPENDA whose function is to collect data on PKB (pajak kendaraan bermotor) and BBNKB (bea balik nama kendaraan bermotor) which manage the data computerized. The purpose of this study is to carry out a security audit of SIMKA BAPENDA at the Badan Pendapatan Daerah Jawa Barat Kota Bandung III using the COBIT 5 framework and ISO/IEC 27002 to document audit findings of the information system audit of the Badan Pendapatan Daerah Jawa Barat Kota Bandung III to make a report on the audit results. Based on the results of research that has been done through interviews and questionnaires using framework and using the APO13 and DSS05 sub domains, the results show that the Capability Existing is at level 1 while Capability Level is level 3 so the Capability Gap is 2.

Keywords: Information Systems, System Security, Digital security, COBIT 5, APO13

1. Introduction

The current digital era where everything is based on high technology, the number of people accessing the digital world is very large and unlimited. But regardless of the many who access digital are good users, because all security holes can be exploited profitably from data theft, to system theft. Therefore, every individual or organization must be able to sort and choose which ones are good and which are not, besides that they can be responsible for personal safety in the digital world. The efforts of each individual, organization and expert continue to strive for digital security that can protect individual or organizational privacy, because the role of digital security is very important for all who use it. Digital security or cybersecurity is security activity against telematics resources. The use of digital security itself serves to secure telematics resources (Yudhiyati et al., 2021; Marune and Hartanto, 2021; Syarie, 2022).

Digital security is used in particular to protect information from computer crime or cyber attacks. Typically, cyberattacks occur because someone wants to logically or physically intervene in a system to compromise the confidentiality, integrity, and availability of information. In this all-digital society, they can meet via the Internet. However, all the ways that can be done by cybercriminals to carry out their attacks and generate profits are of course illegal. Regardless of ethics, cybercriminals target billions of people who care about and have an important role in responding to the pandemic, such as government agencies and other related institutions such as hospitals. They also target companies whose employees have been forced to work from home due to the pandemic by exploiting network security vulnerabilities (Marwan, 2022; Marwan and Bonfigli, 2022; Sensuse et al., 2022).

The West Java Regional Revenue Agency for the City of Bandung III has an archiving system that implements access rights that have been adjusted to their duties and responsibilities, but they still often experience failures such as data leaks due to frequent sharing of access rights with other people, resulting in these access rights being used arbitrarily. by irresponsible people. Based on the results of the author's analysis, the Bapenda Archival Information System or abbreviated as SIMKA BAPENDA is an application or system that summarizes the process from start to finish regarding the management of archival data regarding PKB (pajak kendaraan bermotor)/(motor vehicle tax) and BBNKB (bea balik nama kendaraan bermotor) / (motorized vehicle transfer fee) which functions to managing

physical data into digital data is done using a scannerphysical data results the scanned will be stored in database SIMKA BAPENDAThis digital data will also be stored in database as filing reports on PKB and BBNKB from the West Java Regional Revenue Agency, Bandung City III.

The archival information system in West Java BAPENDA must be protected in such a way as not to be disturbed from threatening virus attacks or people who are not responsible for the security of stored data besides that for the sake of realizing archive management with better archive management, if left alone and there is no follow-up to be corrected they are worried that it will disrupt the continuity of archive data and create a feeling of distrust among users (Prasetyo et al., 2016; Hakim et al., 2021; Romli et al., 2019). For this reason, an audit is needed to get an overview of how to control the security of archival information systems in West Java BAPENDA.

ISMS (information system security management system) is a management process that is structured based on the approach of business risk in planning (Plan), implementing and carrying out operations (Do), monitoring and reviewing (Check) and carrying out security maintenance and improvement (Act)information. The relationship between ISMS and Information Technology in implementing information security cannot be separated. In a sense, if an organization wants to consider information security, it must understand the ISMS implementation process (Sarno and Iffano, 2009). In developing the ISMS adopts the PDCA (Plan – Do – Check -Act) cycle.

To do this, researchers conducted an information system security audit at SIMKA BAPENDA using the Framework COBIT 5 and Standard ISO/IEC 27002 where COBIT 5 is a comprehensive framework that assists companies in achieving goals and generating value through effective information technology governance and management. In addition, the author uses the ISO/IEC 27002 Standard as a reference which was chosen with the consideration that this standard is very flexible so that it can be developed according to organizational needs.

2. Literature Review

2.1. Audit

According to Mulyadi (2016: 8) audit is a systematic process to objectively obtain and evaluate evidence regarding statements about economic activities and events, with the aim of determining the degree of conformity between these statements and predetermined criteria, as well as the delivery of the results. to interested users, from the point of view of the public accounting profession, an audit is an objective examination of the financial statements of a company or other organization with the aim of determining whether the financial statements present fairly, in all material respects, the financial position and results of operations of the company or the organization.

According Arens, Elder, & Beasley (2012): *"Auditing is the accumulation and evaluation of evidence aboutinformation todetermine and report on the degree of correspondencebetween the information and established criteria. Auditing should bedone by a competent, independent person.". Beside Gramling, Johnstone, & Rittenberg (2012): "Systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the result to interested users".*

2.2. Information System Security

Information System Security according to GJ Simons is how we can prevent fraud (cheating) or at least, detect fraud in an information-based system, where the information itself has no physical meaning.

According to (Whitman and Mattord, 2010) information security is a form of protection of information and important elements in it such as confidentiality, integrity, and availability, including systems and hardware for storing and sending that information. Three important elements of information security are:

1. Confidentiality is an element to ensure that information can only be accessed by parties who have the authority to access certain information.
2. Integrity Integrity is an element that ensures that the quality, integrity and completeness of data is maintained according to the authenticity of the data.
3. Availability Confidentiality is an element that ensures that parties who have access rights to an information can access the information in the form needed without interference or obstacles.

According to (ISO/IEC/IEC27002, 2013) regarding Information Security Management System. Information Security has security controls that are useful as an effort to protect against various kinds of threats, ensure business continuity and minimize business risks and can increase investment and business opportunities.

2.3. COBIT 5

According to ISACA (2014) COBIT 5 is one of the business frameworks for governance and management of IT companies. This evolutionary version incorporates the latest thinking in corporate governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust, and value of information systems.

COBIT 5 for Information Security as described in Figure 1 is part of COBIT 5 as a whole, where the focus on COBIT 5 for Information Security is more emphasis on information security and provides a detailed and practical description of guidelines for information security professionals and those who is part of an enterprise that has an interest in the field of information security. In general, I can say the meaning of COBIT 5 is a framework or framework that provides services to enterprises, be it a company, organization or government in managing and managing IT assets or resources to achieve these enterprise goals.

2.4. APO13

The description of the APO13 process is to define, operate and oversee systems for information security management. The purpose of this process is to keep the impact and occurrence of information security incidents at a risk level that is acceptable to the company (ISACA, 2021). Key management practices in APO13 include:

1. APO13.01. Establish and maintain an information security management system (ISMS), which provides an ongoing standard for information security management, secure technology and business processes that suit the business needs and security management of the organization. The essence of this point is to establish and maintain an Information Security Management System.
2. APO13.02 - Define and manage an information security risk Treatment plan, which aims to maintain an information security plan that describes how information security risks are aligned with the organization's strategy and architecture. Define and manage an information security response plan.
3. APO13.03 – Monitor and review the ISMS, aims to collect and analyze data about the ISMS and improve the effectiveness of the ISMS. Monitor and review the Information Security Management System.

2.5. DSS05

According to ISACA (2014) COBIT 5 is one of the business frameworks for governance and management of IT companies. This evolutionary version incorporates the latest thinking in corporate governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust, and value of information systems.

COBIT 5 for Information Security as described in Figure 1 is part of COBIT 5 as a whole, where the focus on COBIT 5 for Information Security is more emphasis on information security and provides a detailed and practical description of guidelines for information security professionals and those who is part of an enterprise that has an interest in the field of information security. In general, I can say the meaning of COBIT 5 is a framework or framework that provides services to enterprises, be it a company, organization or government in managing and managing IT assets or resources to achieve these enterprise goals.

2.6. ISO/IEC 27002

The ISO/IEC 27002 information security standard is the “Code of Practice for

Information Security Management System” in which the standard document contains practical guidelines (code of practice) for information security techniques. ISO 27002 provides best practice recommendations and guidance for organizations on information security management, risks and controls within the context of an Information Security Management System (ISMS). ISO 27002 is a series of ISO 27XXX standard documents provided by the International Standards Organization (ISO) and the International Electronical Commission (IEC) which can be used in handling information security (ISO/IEC 27002:2005, 2007).

The establishment and implementation of an ISMS depends on the strategic orientation of the organization and can be influenced by a number of aspects including the needs, objectives, general requirements, business processes, size and structure of the organization. The ISMS as specified in ISO/IEC 27001 as a whole is an integrated part of the organizational processes and management structure, with the main objective of ensuring the level of confidentiality, integrity and availability of information. To achieve the objectives of the ISMS by implementing a risk management process that supports the ISMS by implementing an information security control suite as part of risk maintenance within the framework of a coherent management system (Carlstedt and Halili, 2016).

3. Materials and Methods

3.1. Materials

Materialas icluding: object, location, data & informations, and tolls used in data analysis. (TN Roman 11pt)

This method contains the Regional Revenue Agency of West Java City of Bandung III. Statements made in the questionnaire refer to the COBIT 5 framework focusing on the APO13 (Manage security) and DSS05 (Manage security) domains. The maturity level assessment of the questionnaire results is based on process capability level consisting of levels 1-5. The scale for measuring data from the questionnaire results used is the Guttman with a yes or no answer.

The questionnaire will be prepared based on COBIT 5 process APO13 and DSS05, which consists of the following questionnaires:

a. APO13.1: Establish and maintain an Information Security Management System.
b. APO13.2: Define and manage an information security response plan
c. APO13.3: Monitor and review the Information Security Management System.
d. DSS05.01: Protects against Malware and manages network security and connectivity.
e. DSS05.02: Manage endpoint security
f. DSS05.03: Manage user identity and logical access.
g. DSS05.04: Manage physical access to IT assets.
h. DSS05.05: Manage sensitive documents and output devices.

This questionnaire is a tool to help collect data based on the APO13 and DSS05 domains in COBIT 5 studied.

3.2. Methods

Methods include: the stages and formulas that are used in data analysis, arranged sequentially step by step.

This study uses a qualitative descriptive data analysis technique that emphasizes data sources and facts. Data collection method with two data sources, namely primary data and secondary data. Based on the data that has been collected through observation, questionnaires and literature studies, the next step is to analyze the data for further development. All data obtained at the Regional Revenue Agency of West Java City of Bandung III were analyzed using the Guttman and Capability Level.scale

Guttman used to analyze respondents' answers to the questionnaire. Respondents' answers consisted of yes answers with a value of 1 or no value of 0. From the results of the Guttman were re-analyzed using a capability level with reference to COBIT 5.

In this study, the research method used is a qualitative descriptive approach. A qualitative descriptive approach was used to get a clear picture of the condition of information system security based on COBIT 5 and ISO/IEC 27002 The data collection carried out in this study was data obtained from interviews and observations regarding the level of information system security capability at SIMKA

BAPENDA. This qualitative descriptive research is also used as a tool to analyze information regarding the performance of the running system, which is then linked to existing theories in the COBIT 5 framework and ISO/IEC 27002 Standards.

4. Results and Discussion

4.1. Result

The results of the evaluation of the implementation of the information system security audit will later contain findings based on the due diligence carried out as well as recommendations to improve the security of the existing BAPENDA SIMKA. The format of the report will vary in each organization because there is no standard format for its preparation. The final report of the audit will present an overview of the current SIMKA BAPENDA security level and then allow the West Java Regional Revenue Agency for the City of Bandung III to take the necessary steps.

Based on the results of an assessment of the BAPENDA SIMKA security audit at the Regional Revenue Agency of West Java Bandung City III, capability level SIMKA BAPENDA security. In more detail can be seen in Table 1.

Table 1: Rating for Domain APO13

Process Name	**Level 1**	**Level 2**		**Level 3**		**Level 4**		**Level 5**	
APO13	**PA 1.1**	**PA 2.1**	**PA 2.2**	**PA 3.1**	**PA 3.2**	**PA 4.1**	**PA 4.2**	**PA 5.1**	**PA5.2**
Rating by Criteria	76%	71%	50%	85%	46%	50%	65%	80%	67%
Rating Capability	L	L	P	L	P	P	L	L	L
Level Achieved	1	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!

The table above shows the rating in domain 13 showing level 1 on PA 1.1 resulting in a rating by criteria of 76% with a rating in category L. An explanation is given in Table 2.

Table 2: Rating for Domain DSS05

Process Name	Level 1	Level 2		Level 3		Level 4		Level 5	
DSS05	**PA 1.1**	**PA 2.1**	**PA 2.2**	**PA 3.1**	**PA 3.2**	**PA 4.1**	**PA 4.2**	**PA 5.1**	**PA5.2**
Rating by Criteria	69%	46%	50%	55%	42%	71%	45%	50%	67%
Rating	L	P	P	L	P	L	P	P	L
Capability Level Achieved	1	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!

The Table 2 above shows the rating on the DSS05 domain showing level 1 on PA 1.1 resulting in a rating by criteria of 69% with a rating in the L category.

5. Discussion

Table 1 shows the rating in domain 13 showing that level 1 at PA 1.1 produces *a rating by criteria* of 76% with *a rating* in category L with *the capability level achieved* at level 1, then level 2 at PA 2.1 produces *a rating by criteria* of 71% with *a rating* in the category L with *the capability level achieved* with the description *STOP!*, level 2 at PA 2.2 produces a rating *by criteria* of 50% with a rating in the P category with the *capability level achieved* with the description *STOP!*, level 3 at PA 3.1 produces a rating *by criteria* of 85% with *a rating* in the L category with *the capability level achieved* with the description *STOP!*, level 3 on PA 3.2 produces a rating by criteria of 46% with a rating in the P category with the capability level achieved with the description , level 2 on PA 4.1 produces *a rating by criteria* of 50% with a rating in the P category with the capability level achieved with the description STOP!, level 4 at PA 4.2 produces a rating by criteria of 65% with a rating in category L with the capability level achieved with the description STOP!, level 5 at PA 5.1 produces a rating by criteria of 80% with a rating in category L with the capability level achieved with the description STOP!, and finally the assessment level 5 on PA 5.2 produces a rating by criteria of 67% with a rating in the L category with the capability level achieved with the description STOP!.

Table 2 shows the rating in the DSS05 domain, showing that level 1 at PA 1.1 produces a rating by criteria of 69% with a rating in category L with the capability level achieved at level 1, then level 2 at PA 2.1 produces a rating by criteria of 46% with a rating in the category P with the capability level achieved with the description STOP!, level 2 on PA 2.2 produces a rating by criteria of 50% with a rating in the P category with the capability level achieved with the description STOP!, level 3 on PA 3.1 produces a rating by criteria of 55% with a rating in the L category with the capability level achieved with the description STOP!, level 3 on PA 3.2 produces a rating by criteria of 42% with a rating in the P category with the capability level achieved with the description STOP!, level 4 on PA 4.1 produces a rating by criteria of 71% with a rating in the L category with the capability level achieved with the description STOP!, level 4 at PA 4.2 produces a rating by criteria of 45% with a rating in the P category with the capability level achieved with the description STOP!, level 5 at PA 5.1 produces a rating by criteria of 50% with a rating in the P category with the capability level achieved with the description STOP!, and finally the assessment level 5 on PA 5.2 produces a rating by criteria of 67% with a rating in the L category with the capability level achieved with the description STOP!.

6. Conclusion

Based on the results of the SIMKA BAPENDA security audit at the West Java Regional Revenue Agency, Bandung City, the following conclusions were obtained:

a. Whereas conducting an audit in this study there were several stages, namely providing background, problem formulation, problem objectives, literature review, audit preparation, audit implementation, and preparation of audit results.
b. Maturity level resulting from the audit and evaluation of the information security management system at SIMKA BAPENDA at the West Java Regional Revenue Agency, Bandung City III obtained through the conditions of the existing domains APO13 and DSS05 obtained level 1 on Capability Existing with the Capability Level expected by the company to be at level 3 Therefore, the Capability Gap in these conditions is 2 levels.
   - Achievement of Capability Exisitng on APO13 and DSS05 is at level 1.
   - Capability Level Achieved in each domain obtained from rating by criteria where domain APO13 withby criteria 76% - Largely achieved (Mostly achieved), and DSS05 with ratingby criteria 69% - Largely achieved (Mostly achieved) placing the SIMKA BAPENDA information system security at level 1, namely Performed Process - The process is executed (one attribute); The implemented process achieves its goals.
c. Generate recommendations for the safety of SIMKA in the West Java Regional Revenue Agency, Bandung City III, such as: - To review and evaluate information about the presence of 106 new threat.
   - In order to conduct regular training about the dangers of malware.
   - To carry out periodic testing for the adequacy of the protection system.

- To communicate the nature and characteristics of potential security related incidents so that they can be easily recognized and their impact understood to enable a commensurate response.
- In order to identify all information processing activities with functional roles, coordinate with business units.
- To conduct regular training on physical safety awareness.

References

Arens, Elder, dan Beasley. 2012. Auditing and Assurance Services, An Integrated Approach. Inggris : Pearson Education Limited.

Carlstedt, A. dan Halili, R. (2016) Whitepaper ISO/IEC 27002:2013 *wartonah*. PECB. Tersedia pada: www.pecb.com

Hakim, R., Umam, K., & Anwar, H. S. (2021). Implementation of E-government through the Samsat mobile Jawa barat at the regional revenue agency of West Java province. *Publica: Jurnal Pemikiran Administrasi Negara, 13*(2), 134-148.

ISACA, W., & Join, R. G. (2021). *Cybersecurity Workforce Diversity—Including Cultures, Personalities and Neurodiversity*.

ISACA. 2014. COBIT 5: *A Business Framework for Governance & Management*. USA: IT Governance Institute.

Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. *International Journal of Business, Economics, and Social Development, 2*(4), 143-152.

Marwan, A., & Bonfigli, F. (2022). Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia. *Bestuur, 10*(1), 22-32.

Marwan, A., Jiow, H. J., & Monteiro, K. (2022). Cybersecurity Regulation and Governance During the Pandemic Time in Indonesia and Singapore. *International Journal of Global Community, 5*(1), 13-32.

Mulyadi. (2016). *Sistem Informasi Akuntansi.* Jakarta: Salemba Empat

Prasetyo, Y., Gunawan, S. A., & Maksum, Z. U. (2016). Determination of the water catchment area in Semarang City using a combination of object based image analysis (OBIA) classification, InSAR and Geographic Information System (GIS) methods based on a high-resolution SPOT 6 image and radar imagery. *In IOP Conference Series: Earth and Environmental Science, 47*(1), p. 012027). IOP Publishing.

Romli, K., Oktaviannur, M., Rinova, D., & Dharmawan, Y. Y. (2019). Analysis of Tourism Mapping in Lampung Province to Optimize Entrepreneurship Development. *Review of Integrative Business and Economics Research, 8*, 110.

Sensuse, D. I., Putro, P. A. W., Rachmawati, R., & Sunindyo, W. D. (2022). Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology. *Information, 13*(12), 580.

Syarief, E. (2022). Security Concerns in Digital Transformation of Electronic Land Registration: Legal Protection in Cybersecurity Laws in Indonesia. *International Journal of Cyber Criminology, 16*(2), 32-46.

Whitman, M. E., & Mattord, H. J. (2010). *Management of information security, Third Edition*. Boston: Course Technology

Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society, 19*(4), 446-462.